

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-076063
(43)Date of publication of application : 14.03.2000

(51)Int.Cl. G06F 9/06
A63F 13/00
G06F 12/14

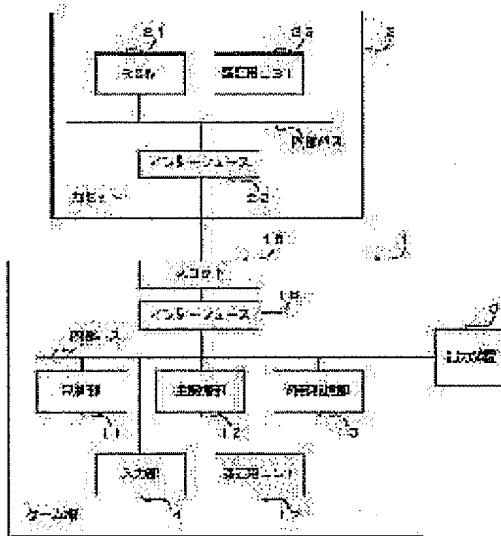
(21)Application number : 10-244762 (71)Applicant : OPEN LOOP:KK
(22)Date of filing : 31.08.1998 (72)Inventor : ASADA KAZUNORI

(54) SYSTEM AND DEVICE FOR CERTIFICATION AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a certification system or the like with which the supply of a game machine and cartridge due to a regular supplier is secured and the read of data or copy of cartridge is blocked.

SOLUTION: A game machine 1 reads the data of a cassette 2 and signature data, for which the digest of these data is enciphered, compares the digest of read data with deciphered signature data and certifies the cassette 2. Next, the cassette 2 returns three digests of challenge data supplied by the game machine 1, digest stored in the cassette itself and common secret data as response data to the game machine 1. The game machine 1 discriminates whether these response data are coincident with three digests of challenge data, deciphered signature data and common secret data stored in the game machine itself or not and certifies the cassette 2. Similarly, the cassette 2 certifies the game machine 1 as well and afterwards, the game machine 1 executes a program stored in the cassette 2.



*** NOTICES ***

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1]An authentication system characterized by what it is [a thing] characterized by comprising the following.

The main part side authentication section.

Have the cartridge side authentication section and said main part side authentication section, The cartridge side signature data is acquired from the main part side memory measure which memorizes the main part side signature data peculiar to self, and said cartridge side authentication section, When it distinguishes whether the cartridge side signature data is peculiar to said cartridge side authentication section and distinguishes that it is peculiar, Have the main part side discriminating means which acquires transfer object data from said cartridge side authentication section, and said cartridge side authentication section, A memory measure which memorizes said transfer object data, and the cartridge side memory measure which memorizes said cartridge side signature data, When said main part side signature data is acquired from said main part side authentication section, it distinguishes whether the main part side signature data is peculiar to said main part side authentication section and it distinguishes that it is peculiar, The cartridge side discriminating means which supplies said transfer object data which said memory measure has memorized to said main part side authentication section.

[Claim 2]Said cartridge side signature data expresses what enciphered a digest which expresses a predetermined value assigned to a tropism function on the other hand for specific data using a secret key, Said cartridge side memory measure is provided with a means to memorize said specific data, and said main part side authentication section, Acquire said specific data from said cartridge side authentication section, and said cartridge side signature data is decrypted using a public key, When it distinguishes whether said decrypted cartridge side signature data is substantially the same as said digest and distinguishes substantially that it is the same, The authentication system according to claim 1 characterized by what it is distinguished for whether said cartridge side signature data is peculiar to said cartridge side authentication section.

[Claim 3]Said specific data consists of a portion beforehand specified among said transfer object data, and said cartridge side memory measure, Have a means to memorize identification data for a signature which specifies said portion, and said main part side authentication section, The authentication system according to claim 2 characterized by what it has a means to acquire said portion specified with said identification data for a signature which acquired said identification data for a signature and was acquired from said cartridge side memory measure among said transfer object data as said specific data for.

[Claim 4]Said portion specified with said identification data for a signature, The authentication system according to claim 3 characterized by what is chosen so that the time required until it distinguishes whether said cartridge side signature data decrypted after said main part side authentication section acquired said specific data is substantially the same as said digest may become in less than fixed time.

[Claim 5]The authentication system according to claim 2, 3, or 4 characterized by what said main part side authentication section is provided with a key memory measure which memorizes said

public key supplied from the outside so that rewriting is possible, and said cartridge side signature data is decrypted for using said public key which said key memory measure memorizes.

[Claim 6]An authentication system given in any 1 paragraph of claims 2 thru/or 5 characterized by what it is [a thing] characterized by comprising the following.

A means for said main part side memory measure and said cartridge side memory measure to be provided with a means to memorize the same common restricted data of each other substantially, respectively, and for said main part side discriminating means to create the main part side challenge data, and to supply said cartridge side discriminating means.

The cartridge side challenge data are acquired from said cartridge side discriminating means, The acquired cartridge side challenge data, A means to create the main part side response data which expresses said value assigned to a tropism function on the other hand for data showing three persons of said common restricted data which said decrypted cartridge side signature data and said main part side memory measure memorize, and to supply said cartridge side discriminating means.

The cartridge side response data is acquired from said cartridge side discriminating means, It is distinguished whether said value assigned to a tropism function on the other hand expresses said cartridge side response data for data showing three persons of said common restricted data which said main part side challenge data, said decrypted cartridge side signature data, and said main part side memory measure memorize, When are expressed and it distinguishes, have a means to distinguish that said cartridge side signature data is peculiar to said cartridge side authentication section, and said cartridge side memory measure, A means for it to have a digest memory measure which memorizes said digest, and for said cartridge side discriminating means to create said cartridge side challenge data, and to supply said main part side discriminating means.

Said main part side challenge data which acquired and acquired said main part side challenge data from said main part side discriminating means, Said cartridge side response data which expresses said value assigned to a tropism function on the other hand for data showing three persons of said common restricted data which said digest which said cartridge side memory measure memorizes, and said cartridge side memory measure memorize is created. Said main part side response data is acquired from a means to supply said main part side discriminating means, and said main part side discriminating means, Said cartridge side challenge data, When it distinguished and meant whether said value assigned to a tropism function on the other hand would express said main part side response data for data showing three persons of said common restricted data which said digest which said cartridge side memory measure memorizes, and said cartridge side memory measure memorize and distinguishes, A means to distinguish that said main part side signature data is peculiar to said main part side authentication section.

[Claim 7]The authentication system according to claim 6 characterized by what said digest memory measure is provided with a means to memorize substantially said digest supplied from the outside in un-volatilizing for.

[Claim 8]Said memory measure is provided with a means to memorize said enciphered transfer object data, and said main part side authentication section, When it distinguishes that the cartridge side signature data acquired from said cartridge side authentication section is peculiar to said cartridge side authentication section, An authentication system given in any 1 paragraph of claims 2 thru/or 7 characterized by what it has a means to acquire said enciphered transfer object data from said cartridge side authentication section, and to decrypt it for.

[Claim 9]Said memory measure is provided with a means to match said enciphered transfer object data with signature data for encryption data peculiar to the enciphered transfer object data concerned, and to memorize it, When said main part side authentication section distinguishes that the cartridge side signature data acquired from said cartridge side authentication section is peculiar to said cartridge side authentication section, Said signature data for encryption data is acquired from said cartridge side authentication section, When it distinguishes whether said acquired signature data for encryption data is peculiar to said transfer

object data enciphered [which was matched with the signature data for encryption data concerned] and distinguishes that it is peculiar, The authentication system according to claim 8 characterized by what it has a means to acquire and decrypt said transfer object data enciphered [which was matched with the signature data for encryption data concerned] for, [Claim 10] Said memory measure is provided with a means to memorize position data which identifies a logical position of a portion which memorizes said enciphered transfer object data among storage areas which self has, Said specific data contains the position data concerned, and said main part side authentication section, The authentication system according to claim 8 or 9 characterized by what it has a means to acquire and decrypt said enciphered transfer object data from a logical position identified with said position data among storage areas which said memory measure has for.

[Claim 11] The authentication system according to claim 8 or 9 characterized by what it is [a thing] characterized by comprising the following.

A means to memorize position data which identifies a logical position of a portion which memorizes said enciphered transfer object data among storage areas where self has said memory measure.

A means to memorize signature data for position data peculiar to said position data.

A preparation and said main part side authentication section acquire said signature data for position data from said cartridge side authentication section, and it is distinguished whether said acquired signature data for position data is peculiar to said position data, A means to acquire and decrypt said enciphered transfer object data from a logical position identified with said position data among storage areas which said memory measure has when it distinguishes that it is peculiar.

[Claim 12] A memory measure which memorizes transfer object data.

The cartridge side memory measure which memorizes specific data and the cartridge side signature data showing what enciphered a digest which expresses a predetermined value assigned to a tropism function on the other hand for the specific data concerned using a secret key.

The cartridge side discriminating means which supplies said transfer object data which said memory measure has memorized to the device concerned when the main part side signature data is acquired from a device connected to self, it distinguishes whether the main part side signature data is peculiar to the device concerned and it distinguishes that it is peculiar.

The main part side memory measure which is the authentication device provided with the above and memorizes said main part side signature data peculiar to self, Acquire said specific data from said cartridge side authentication device, and said cartridge side signature data is decrypted using a public key, When it distinguishes whether said decrypted cartridge side signature data is substantially the same as said digest and distinguishes substantially that it is the same, it has the main part side discriminating means which acquires said transfer object data from said cartridge side authentication device.

[Claim 13] The main part side memory measure which memorizes the main part side signature data peculiar to self characterized by comprising the following, Said cartridge side signature data and said specific data are acquired from a device which memorizes specific data and the cartridge side signature data showing what enciphered a digest which expresses a predetermined value assigned to a tropism function on the other hand for the specific data concerned using a secret key, Decrypt said acquired cartridge side signature data using a public key, and it is distinguished whether said decrypted cartridge side signature data is substantially the same as said digest, An authentication device connected to the main part side authentication device provided with the main part side discriminating means which acquires transfer object data from said device when it distinguishes substantially that it is the same removable.

A memory measure which memorizes said transfer object data.

The cartridge side memory measure which memorizes said cartridge side signature data and said specific data, When said main part side signature data is acquired from said main part side

authentication device, it distinguishes whether the main part side signature data is peculiar to said main part side authentication device and it distinguishes that it is peculiar, The cartridge side discriminating means which supplies said transfer object data which said memory measure has memorized to said main part side authentication device.

[Claim 14]Have the 1st and 2nd authentication sections and said 1st authentication section, Specific data is acquired from the 1st memory measure that memorizes the 1st signature data peculiar to self, and said 2nd authentication section, Decrypt the 2nd signature data using a public key, and it is distinguished whether said 2nd decrypted signature data is substantially the same as a digest which expresses a predetermined value assigned to a tropism function on the other hand for specific data, When it distinguishes substantially that it is the same, and distinguishes whether said 2nd signature data is peculiar to said 2nd authentication section and distinguishes that it is peculiar, Have the 1st discriminating means that acquires transfer object data from said 2nd authentication section, and said 2nd authentication section, The 2nd memory measure that memorizes said transfer object data and said 2nd signature data, When said 1st signature data is acquired from said 1st authentication section, it distinguishes whether the 1st signature data is peculiar to said 1st authentication section and it distinguishes that it is peculiar, Have the 2nd discriminating means that supplies said transfer object data which said 2nd memory measure has memorized to said 1st authentication section, and said 2nd signature data, An authentication system characterized by what what enciphered a predetermined value assigned to a tropism function on the other hand using a secret key for said specific data showing a portion as which it was beforehand specified of said transfer object data is expressed for.

[Claim 15]Said 2nd memory measure is provided with a means to memorize said enciphered transfer object data, and said 1st authentication section, The authentication system according to claim 14 characterized by what it has a means to acquire said enciphered transfer object data from said 2nd authentication section, and to decrypt it for when it distinguishes that the 2nd signature data acquired from said 2nd authentication section is peculiar to said 2nd authentication section.

[Claim 16]Said 2nd memory measure is provided with a means to match said enciphered transfer object data with signature data for encryption data peculiar to the enciphered transfer object data concerned, and to memorize it, When said 1st authentication section distinguishes that the 2nd signature data acquired from said 2nd authentication section is peculiar to said 2nd authentication section, Acquire said signature data for encryption data from said 2nd authentication section, and said acquired signature data for encryption data, When it distinguishes whether it is peculiar to said transfer object data enciphered [which was matched with the signature data for encryption data concerned] and distinguishes that it is peculiar, The authentication system according to claim 15 characterized by what it has a means to acquire and decrypt said transfer object data enciphered [which was matched with the signature data for encryption data concerned] for.

[Claim 17]The main part side memory measure which memorizes said main part side signature data peculiar to self for a computer connected to the cartridge side authentication device removable, comprising, Acquire said specific data from said cartridge side authentication device, and said cartridge side signature data is decrypted using a public key, When it distinguishes whether said decrypted cartridge side signature data is substantially the same as said digest and distinguishes substantially that it is the same, A recording medium which recorded a program for considering it as the main part side discriminating means which acquires said transfer object data from said cartridge side authentication device, and making it function and in which computer reading is possible.

A memory measure which memorizes transfer object data.

The cartridge side memory measure which memorizes specific data and the cartridge side signature data showing what enciphered a digest which expresses a predetermined value assigned to a tropism function on the other hand for the specific data concerned using a secret key, The cartridge side discriminating means which supplies said transfer object data which said

memory measure has memorized to the device concerned when the main part side signature data is acquired from a device connected to self, it distinguishes whether the main part side signature data is peculiar to the device concerned and it distinguishes that it is peculiar.

[Claim 18]A memory measure which memorizes said transfer object data for a computer connected to the main part side authentication device characterized by comprising the following removable, The cartridge side memory measure which memorizes said cartridge side signature data and said specific data, When said main part side signature data is acquired from said main part side authentication device, it distinguishes whether the main part side signature data is peculiar to said main part side authentication device and it distinguishes that it is peculiar, A recording medium which recorded a program for making said transfer object data which said memory measure has memorized into the cartridge side discriminating means supplied to said main part side authentication device, and operating it and in which computer reading is possible. The main part side memory measure which memorizes the main part side signature data peculiar to self.

Said cartridge side signature data and said specific data are acquired from a device which memorizes specific data and the cartridge side signature data showing what enciphered a digest which expresses a predetermined value assigned to a tropism function on the other hand for the specific data concerned using a secret key, Decrypt said acquired cartridge side signature data using a public key, and it is distinguished whether said decrypted cartridge side signature data is substantially the same as said digest, The main part side discriminating means which acquires transfer object data from said device when it distinguishes substantially that it is the same.

[Translation done.]

*** NOTICES ***

JPO and INPI are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]**[0001]**

[Field of the Invention]Especially this invention relates to the authentication system and authentication device for restricting the user and supplier of data about an authentication system and an authentication device.

[0002]

[Description of the Prior Art]When a game machine provides a user with a game, Usually, a game machine is equipped with the cartridge containing memory storage, such as ROM (Read Only Memory) which stored the game program, A game machine reads the program data of a game program from the memory storage of a cartridge, and is made to execute the game program.

[0003]

[Problem(s) to be Solved by the Invention]However, for the purpose of maintaining the quality of the game supplied to a commercial scene for consumer protection, to restrict the supplier of a game to the person of the fixed range, it is necessary to prevent a game from being supplied by those who have not got permission of game supply. However, supply of the game ungranted a permission cannot be prevented in an above-mentioned technique.

[0004]The above-mentioned situation is the same also about a game machine body. That is, even if it is a case where supply of the game machine ungranted a permission needs to be prevented for the consumer protection by the quality maintenance of a game machine, supply of the game machine ungranted a permission cannot be prevented in an above-mentioned technique.

[0005]Even if it is the cartridge supplied by the regular game supplier, by reproducing the cartridge unjustly, there is a risk of the cartridge which is not what was purchased regularly circulating, and the unjust duplicate of a cartridge cannot be prevented by an above-mentioned technique.

[0006]Even if it does not result in the duplicate of the whole cartridge, there is danger of the data stored in the memory storage of a cartridge being read unjustly, and being analyzed. And if the memory storage is built into a cartridge after the data read unjustly is stored in memory storage, two or more games will come to be unjustly performed after all using a common cartridge.

[0007]When the read data has commodity value independently, even if it is a case where a game is unreproducible from the data (for example, when the data is image data), a risk of the data circulating independently is large.

[0008]It was made in view of the above-mentioned actual condition, supply of the game machine by a regular supplier and a cartridge is secured, and an object of this invention is to provide the authentication system and authentication device with which read-out of data and the duplicate of a cartridge are prevented.

[0009]

[Means for Solving the Problem]In order to attain the above-mentioned purpose, an authentication system concerning the 1st viewpoint of this invention, Have the main part side authentication section and the cartridge side authentication section, and said main part side

authentication section, The cartridge side signature data is acquired from the main part side memory measure which memorizes the main part side signature data peculiar to self, and said cartridge side authentication section, When it distinguishes whether the cartridge side signature data is peculiar to said cartridge side authentication section and distinguishes that it is peculiar, Have the main part side discriminating means which acquires transfer object data from said cartridge side authentication section, and said cartridge side authentication section, A memory measure which memorizes said transfer object data, and the cartridge side memory measure which memorizes said cartridge side signature data, When said main part side signature data is acquired from said main part side authentication section, it distinguishes whether the main part side signature data is peculiar to said main part side authentication section and it distinguishes that it is peculiar, It has the cartridge side discriminating means which supplies said transfer object data which said memory measure has memorized to said main part side authentication section.

[0010]According to such an authentication system, the main part side authentication section and the cartridge side authentication section send and receive transfer object data, after attesting that each other is manufactured regularly. Therefore, it is prevented from those who are allowed neither creation of the cartridge side signature data, nor acquisition of a secret key that transfer object data is supplied.

[0011]Said cartridge side signature data expresses what enciphered a digest which expresses a predetermined value assigned to a tropism function on the other hand for specific data, for example using a secret key, In this case, said cartridge side memory measure is provided with a means to memorize said specific data, and said main part side authentication section, Acquire said specific data from said cartridge side authentication section, and said cartridge side signature data is decrypted using a public key, When it distinguishes whether said decrypted cartridge side signature data is substantially the same as said digest and distinguishes substantially that it is the same, It may be distinguished whether said cartridge side signature data is peculiar to said cartridge side authentication section. Thereby, since the main part side authentication section verifies the justification of the cartridge side signature data first, danger of unjust supply of transfer object data decreases further.

[0012]Said specific data consists of a portion beforehand specified among said transfer object data, and said cartridge side memory measure, Have a means to memorize identification data for a signature which specifies said portion, and said main part side authentication section, It may have a means to acquire said portion specified with said identification data for a signature which acquired said identification data for a signature and was acquired from said cartridge side memory measure among said transfer object data as said specific data. And said portion specified with said identification data for a signature, for example, It is good also as what is chosen so that the time required until it distinguishes whether said cartridge side signature data decrypted after said main part side authentication section acquired said specific data is substantially the same as said digest may become in less than fixed time. Time required by this in order that the main part side authentication section may check the identity of the cartridge side signature data and a digest is stopped short, and transmission of transfer object data is performed smoothly.

[0013]If said main part side authentication section shall be provided with a key memory measure which memorizes said public key supplied from the outside so that rewriting is possible and said cartridge side signature data shall be decrypted using said public key which said key memory measure memorizes, The main part side authentication section needs to be individually manufactured as a thing for attesting each cartridge side authentication section, where a memory content of a key memory measure is initialized, it will mass-produce the main part side authentication section, for example, and it should just write a public key in a key memory measure behind.

[0014]Said main part side memory measure and said cartridge side memory measure, For example, have a means to memorize the same common restricted data of each other substantially, respectively, and in this case said main part side discriminating means, For example, a means to create the main part side challenge data and to supply said cartridge side

discriminating means, The cartridge side challenge data are acquired from said cartridge side discriminating means, The acquired cartridge side challenge data, A means to create the main part side response data which expresses said value assigned to a tropism function on the other hand for data showing three persons of said common restricted data which said decrypted cartridge side signature data and said main part side memory measure memorize, and to supply said cartridge side discriminating means, The cartridge side response data is acquired from said cartridge side discriminating means, It is distinguished whether said value assigned to a tropism function on the other hand expresses said cartridge side response data for data showing three persons of said common restricted data which said main part side challenge data, said decrypted cartridge side signature data, and said main part side memory measure memorize, By having a means to distinguish that said cartridge side signature data is peculiar to said cartridge side authentication section, when are expressed and it distinguishes, It attests that the cartridge side authentication section is manufactured regularly. And said cartridge side memory measure is provided with a digest memory measure which memorizes said digest, and said cartridge side discriminating means, For example, a means to create said cartridge side challenge data and to supply said main part side discriminating means, Said main part side challenge data which acquired and acquired said main part side challenge data from said main part side discriminating means, Said cartridge side response data which expresses said value assigned to a tropism function on the other hand for data showing three persons of said common restricted data which said digest which said cartridge side memory measure memorizes, and said cartridge side memory measure memorize is created. Said main part side response data is acquired from a means to supply said main part side discriminating means, and said main part side discriminating means, Said cartridge side challenge data, When it distinguished and meant whether said value assigned to a tropism function on the other hand would express said main part side response data for data showing three persons of said common restricted data which said digest which said cartridge side memory measure memorizes, and said cartridge side memory measure memorize and distinguishes, By having a means to distinguish that said main part side signature data is peculiar to said main part side authentication section, It attests that the main part side authentication section is manufactured regularly.

[0015]If it shall have a means to memorize substantially said digest supplied from the outside in un-volatilizing, said digest memory measure the cartridge side authentication section, What is necessary will be to be individually manufactured for every thing from which transfer object data to memorize differs, to mass-produce the cartridge side authentication section, where a memory content of a means to memorize a digest in un-volatilizing is initialized for example, and just to write a digest in the cartridge side authentication section behind.

[0016]Said memory measure is provided with a means to memorize said enciphered transfer object data, and said main part side authentication section, When it distinguishes that the cartridge side signature data acquired from said cartridge side authentication section is peculiar to said cartridge side authentication section, it may have a means to acquire said enciphered transfer object data from said cartridge side authentication section, and to decrypt it.

[0017]Thereby, about enciphered transfer object data, the privacy improves further. If a portion which has on utility value of the data concerned among transfer object data is enciphered at a vermin ceremony, efficiency of transmission of data will also be kept high.

[0018]Said memory measure is provided with a means to match said enciphered transfer object data with signature data for encryption data peculiar to the enciphered transfer object data concerned, and to memorize it, When said main part side authentication section distinguishes that the cartridge side signature data acquired from said cartridge side authentication section is peculiar to said cartridge side authentication section, Said signature data for encryption data is acquired from said cartridge side authentication section, When it distinguishes whether said acquired signature data for encryption data is peculiar to said transfer object data enciphered [which was matched with the signature data for encryption data concerned] and distinguishes that it is peculiar, It may have a means to acquire and decrypt said transfer object data enciphered [which was matched with the signature data for encryption data concerned].

[0019]Thereby, each transfer object data is individually made into an object of attestation by

signature, therefore propriety of transmission is determined individually. For this reason, the privacy of data improves further and the privacy of a mutually different level is provided according to a difference of the importance of transfer object data of further each, etc.

[0020]Said memory measure is provided with a means to memorize position data which identifies a logical position of a portion which memorizes said enciphered transfer object data among storage areas which self has, Said specific data contains the position data concerned, and said main part side authentication section may be provided with a means to acquire and decrypt said enciphered transfer object data from a logical position identified with said position data among storage areas which said memory measure has.

[0021]As a result of unjust rewriting of position data becoming impossible substantially by this, a risk of it becoming impossible substantially to write enciphered transfer object data in the cartridge side authentication section unjustly, therefore transfer object data being rewritten unjustly is avoided. Since a size of the position data itself is usually small to such an extent that it can be disregarded compared with transfer object data, efficiency of a data transfer is not spoiled.

[0022]A means to memorize position data which identifies a logical position of a portion which memorizes said enciphered transfer object data among storage areas where self has said memory measure, Have a means to memorize signature data for position data peculiar to said position data, and said main part side authentication section, When said signature data for position data is acquired from said cartridge side authentication section, it distinguishes whether said acquired signature data for position data is peculiar to said position data and it distinguishes that it is peculiar, it has a means to acquire and decrypt said enciphered transfer object data from a logical position identified with said position data among storage areas which said memory measure has — a thing may be carried out. As a result of unjust rewriting of position data becoming impossible substantially, a risk of transfer object data being rewritten unjustly is avoided by this.

[0023]An authentication device concerning the 2nd viewpoint of this invention, The cartridge side memory measure which memorizes the cartridge side signature data showing what enciphered a memory measure which memorizes transfer object data, and a digest which expresses a predetermined value assigned to a tropism function on the other hand for specific data and the specific data concerned using a secret key, When the main part side signature data is acquired from a device connected to self, it distinguishes whether the main part side signature data is peculiar to the device concerned and it distinguishes that it is peculiar, The cartridge side discriminating means which supplies said transfer object data which said memory measure has memorized to the device concerned, The main part side memory measure which is an authentication device connected to the ***** cartridge side authentication device removable, and memorizes said main part side signature data peculiar to self, Acquire said specific data from said cartridge side authentication device, and said cartridge side signature data is decrypted using a public key, When it distinguishes whether said decrypted cartridge side signature data is substantially the same as said digest and distinguishes substantially that it is the same, it has the main part side discriminating means which acquires said transfer object data from said cartridge side authentication device.

[0024]Such an authentication device sends and receives transfer object data, after attesting that each other is manufactured regularly between the cartridge side authentication devices. The justification of the cartridge side signature data is also verified. Therefore, it is prevented from those who are allowed neither creation of the cartridge side signature data, nor acquisition of a secret key that transfer object data is supplied.

[0025]An authentication device concerning the 3rd viewpoint of this invention, The main part side memory measure which memorizes the main part side signature data peculiar to self, and specific data, And said cartridge side signature data and said specific data are acquired from a device which memorizes the cartridge side signature data showing what enciphered a digest which expresses a predetermined value assigned to a tropism function on the other hand for the specific data concerned using a secret key, Decrypt said acquired cartridge side signature data using a public key, and it is distinguished whether said decrypted cartridge side signature data is

substantially the same as said digest, The main part side discriminating means which acquires transfer object data from said device when it distinguishes substantially that it is the same, A memory measure which is an authentication device connected to the preparation ***** side authentication device removable, and memorizes said transfer object data, When said main part side signature data is acquired from said main part side authentication device, it distinguishes whether the main part side signature data is peculiar to said main part side authentication device from the cartridge side memory measure which memorizes said cartridge side signature data and said specific data and it distinguishes that it is peculiar, It has the cartridge side discriminating means which supplies said transfer object data which said memory measure has memorized to said main part side authentication device.

[0026]Such an authentication device sends and receives transfer object data, after attesting that each other is manufactured regularly between the main part side authentication devices. The justification of the cartridge side signature data is also verified. Therefore, it is prevented from those who are allowed neither creation of the cartridge side signature data, nor acquisition of a secret key that transfer object data is supplied.

[0027]An authentication system concerning the 4th viewpoint of this invention, Have the 1st and 2nd authentication sections and said 1st authentication section, Specific data is acquired from the 1st memory measure that memorizes the 1st signature data peculiar to self, and said 2nd authentication section, Decrypt the 2nd signature data using a public key, and it is distinguished whether said 2nd decrypted signature data is substantially the same as a digest which expresses a predetermined value assigned to a tropism function on the other hand for specific data, When it distinguishes substantially that it is the same, and distinguishes whether said 2nd signature data is peculiar to said 2nd authentication section and distinguishes that it is peculiar, Have the 1st discriminating means that acquires transfer object data from said 2nd authentication section, and said 2nd authentication section, The 2nd memory measure that memorizes said transfer object data and said 2nd signature data, When said 1st signature data is acquired from said 1st authentication section, it distinguishes whether the 1st signature data is peculiar to said 1st authentication section and it distinguishes that it is peculiar, Have the 2nd discriminating means that supplies said transfer object data which said 2nd memory measure has memorized to said 1st authentication section, and said 2nd signature data, What enciphered a predetermined value assigned to a tropism function on the other hand using a secret key for said specific data showing a portion as which it was beforehand specified of said transfer object data is expressed.

[0028]According to such an authentication system, the 1st and 2nd authentication sections send and receive transfer object data, after attesting that each other is manufactured regularly. Therefore, it is prevented from those who are allowed neither creation of the 2nd signature data, nor acquisition of a secret key that transfer object data is supplied.

[0029]Said 2nd memory measure is provided with a means to memorize said enciphered transfer object data, and said 1st authentication section, When it distinguishes that the 2nd signature data acquired from said 2nd authentication section is peculiar to said 2nd authentication section, it may have a means to acquire said enciphered transfer object data from said 2nd authentication section, and to decrypt it. Thereby, about enciphered transfer object data, the privacy improves further. If a portion which has on utility value of the data concerned among transfer object data is enciphered at a vermin ceremony, efficiency of transmission of data will also be kept high.

[0030]Said 2nd memory measure is provided with a means to match said enciphered transfer object data with signature data for encryption data peculiar to the enciphered transfer object data concerned, and to memorize it, When said 1st authentication section distinguishes that the 2nd signature data acquired from said 2nd authentication section is peculiar to said 2nd authentication section, Acquire said signature data for encryption data from said 2nd authentication section, and said acquired signature data for encryption data, When it distinguishes whether it is peculiar to said transfer object data enciphered [which was matched with the signature data for encryption data concerned] and distinguishes that it is peculiar, It may have a means to acquire and decrypt said transfer object data enciphered [which was matched with the signature data for encryption data concerned]. Thereby, each transfer object

data is individually made into an object of attestation by signature, therefore propriety of transmission is determined individually. For this reason, the privacy of data improves further and the privacy of a mutually different level is provided according to a difference of the importance of transfer object data of further each, etc.

[0031]A recording medium concerning the 5th viewpoint of this invention in which computer reading is possible, The cartridge side memory measure which memorizes the cartridge side signature data showing what enciphered a memory measure which memorizes transfer object data, and a digest which expresses a predetermined value assigned to a tropism function on the other hand for specific data and the specific data concerned using a secret key, When the main part side signature data is acquired from a device connected to self, it distinguishes whether the main part side signature data is peculiar to the device concerned and it distinguishes that it is peculiar, The cartridge side discriminating means which supplies said transfer object data which said memory measure has memorized to the device concerned, The main part side memory measure which memorizes said main part side signature data peculiar to self for a computer connected to the ***** cartridge side authentication device removable, Acquire said specific data from said cartridge side authentication device, and said cartridge side signature data is decrypted using a public key, The main part side discriminating means which acquires said transfer object data from said cartridge side authentication device when it distinguishes whether said decrypted cartridge side signature data is substantially the same as said digest and distinguishes substantially that it is the same, It carried out and a program for making it function was recorded.

[0032]A computer which executes a program recorded on such a recording medium sends and receives transfer object data, after attesting that each other is manufactured regularly between the cartridge side authentication devices. The justification of the cartridge side signature data is also verified. Therefore, it is prevented from those who are allowed neither creation of the cartridge side signature data, nor acquisition of a secret key that transfer object data is supplied.

[0033]A recording medium concerning the 6th viewpoint of this invention in which computer reading is possible, The main part side memory measure which memorizes the main part side signature data peculiar to self, and specific data, And said cartridge side signature data and said specific data are acquired from a device which memorizes the cartridge side signature data showing what enciphered a digest which expresses a predetermined value assigned to a tropism function on the other hand for the specific data concerned using a secret key, Decrypt said acquired cartridge side signature data using a public key, and it is distinguished whether said decrypted cartridge side signature data is substantially the same as said digest, The main part side discriminating means which acquires transfer object data from said device when it distinguishes substantially that it is the same, A memory measure which memorizes said transfer object data for a computer connected to the preparation ***** side authentication device removable, When said main part side signature data is acquired from said main part side authentication device, it distinguishes whether the main part side signature data is peculiar to said main part side authentication device from the cartridge side memory measure which memorizes said cartridge side signature data and said specific data and it distinguishes that it is peculiar, A program for making said transfer object data which said memory measure has memorized into the cartridge side discriminating means supplied to said main part side authentication device, and operating it was recorded.

[0034]A computer which executes a program recorded on such a recording medium sends and receives transfer object data, after attesting that each other is manufactured regularly between the main part side authentication devices. The justification of the cartridge side signature data is also verified. Therefore, it is prevented from those who are allowed neither creation of the cartridge side signature data, nor acquisition of a secret key that transfer object data is supplied.

[0035]

[Embodiment of the Invention]The game system having contained the cassette which memorizes the software for games with which a game machine and its game machine perform the

authentication system and authentication device concerning this embodiment of the invention is explained as an example.

[0036]Drawing 1 is a figure showing the composition of this game system. This game system consists of the game machine 1, the cassette 2, and the output unit 3 so that it may illustrate.

[0037]The game machine 1 consists of the control section 11, the main memory part 12, the external memory part 13, the input part 14, the slot 15, the interface 16, and LSI(Large Scale Integrated circuit) 17 for attestation. The control section 11 is connected to LSI17 the main memory part 12, the external memory part 13, the input part 14, the interface 16, and for attestation via the internal bus, and the interface 16 is connected to the slot 15. The control section 11 is connected to the output unit 3.

[0038]The control section 11 consists of CPUs (Central Processing Unit) etc., and executes the game program which the program data supplied via the interface 16 from the cassette 2 expresses. The control section 11 reads the program data which the external memory part 13 memorizes, and performs the below-mentioned processing in which the program which the program data expresses was followed.

[0039]The main memory part 12 consists of RAM (Random Access Memory) etc., and is used as workspace of the control section 11. The external memory part 13 consists of ROMs (Read Only Memory) etc., and memorizes the program data showing the processing which the control section 11 should perform.

[0040]The input part 14 consists of joy sticks etc., and supplies the signal according to a user's operation to the control section 11. The slot 15 connects mutually the interface 16 of the game machine 1, and the interface 22 of the cassette 2 by equipping with the interface 22 of the cassette 2 removable.

[0041]The interface 16 changes into the data of parallel form the data of the serial form supplied from the interface 22 of the cassette 2, and supplies it to the control section 11 or LSI17 for attestation. The interface 16 changes into the data of serial form the data of the parallel form supplied from the control section 11, and supplies it to the interface 22.

[0042]LSI17 for attestation supplies the digest and random number which were obtained from ASIC (application-specific integrated circuit) etc. by becoming and performing the calculation of a digest and generating of a random number which are mentioned later according to the processing mentioned later to the control section 11. LSI17 for attestation has memorized beforehand the secret key for the below-mentioned key encryption used in order to perform processing mentioned later, the public key for signature verification, and common restricted data.

[0043]The cassette 2 consists of ROM21, the interface 22, and LSI23 for attestation. ROM21 and LSI23 for attestation are connected to the interface 22 via the internal bus. And ROM21 outputs the data which self has memorized according to directions of the control section 11 of the game machine 1. The outputted data is supplied to the control section 11 via the interface 22 of the cassette 2, and the interface 16 of the game machine 1.

[0044]As shown, for example in drawing 2, the information shown as (1) ~ (6) below is stored in ROM21. Namely, the non-enciphering module which is data which expresses a part of game program which the (1) game machine 1 should execute to the storage area of ROM21, and is data in which encryption is not given, (2) The encryption module which is data showing a part of game program which the game machine 1 should execute, and expresses what was enciphered using the predetermined encryption key, (3) The encryption encryption key showing what enciphered the above-mentioned encryption key used in order to create an encryption module (that is, above-mentioned information on (2)) using the public key for predetermined key encryption, (4) The encryption position list showing the information, including for example, the address etc. which were given to the storage area, which pinpoints the storage area where each encryption module is stored among the storage area of ROM21, (5) The list for a signature showing the information, including for example, the address etc. which were given to the storage area, which pinpoints the storage area which is an object of a digital signature among the storage area of ROM21, (6) The signature data and ** showing what enciphered the value (namely, "digest") which substituted for the predetermined hash function what combined the whole data

stored in the storage area which the list for a signature (that is, above-mentioned information on (5)) expresses in accordance with the predetermined rule with the secret key for a signature. It is beforehand stored by the supplier of the cassette 2, etc.

[0045]The encryption key used in order to create the information on (2) may be arbitrary, for example, should just be based on DES (Data Encryption Standard) which is a standard which the United States of America defines. The public key for the key encryption used in order to encipher the encryption key concerned, and the secret key for key decryption which makes a pair are memorized by LSI17 for attestation of the game machine 1. The above-mentioned digest used for creation of the data of (6) should just be created using the arbitrary functions which can be substantially treated as a hash function, and the function concerned should just be based, for example on SHA (Secure Hash Algorithm).

[0046]And the secret key for an above-mentioned signature and the public key for signature verification which makes a pair are memorized by LSI17 for attestation of the game machine 1. However, the secret key for a signature is separate from the secret key for key decryption which becomes a public key for the key encryption used in order to create the information on (3), and a pair.

[0047]The data (namely, data stored in the storage area which the list for a signature shows) made into the object of a digital signature for creation of signature data is beforehand specified by the supply origin of the cassette 2, etc. As a standard which specifies the data of the object of a digital signature, What is necessary is just to specify the data concerned so that the time required after specifically acquiring the data of the object of a digital signature according to the processing which LSI17 for attestation mentions later, for example until it computes the digest of the data concerned may become in less than fixed time. The speed of processing of the signature check mentioned later is maintained by this more than constant speed, therefore a smooth advance of the game by this game system is secured.

[0048]However, let the encryption position list (namely, above-mentioned information on (4)) be an object of a digital signature except for the case where an encryption module says that one piece is not stored in ROM21, either, therefore an encryption position list does not exist.

Therefore, as long as the encryption position list is stored in ROM21, the information which pinpoints the storage area where the encryption position list is stored shall be included in the list for a signature.

[0049]Thus, a risk of the data stored in ROM21 being rewritten unjustly is avoided by making an encryption position list into the contents of the digital signature. That is, in order to verify signature data, the whole data specified with the list for a signature is used so that it may mention later. For this reason, in order to attest the cassette 2 in spite of unjust rewriting of the data stored in ROM21, it will be necessary to leave, without rewriting an encryption position list. Therefore, those who rewrite data unjustly cannot write an encryption module in the storage area which the encryption position list left behind to ROM21 does not show. For this reason, it becomes very difficult to write unjustly the data which has utility value substantially in ROM21.

[0050]The interface 22 changes into the data of parallel form the data of the serial form supplied from the interface 16 of the game machine 1, and supplies it to LSI23 for attestation. The interface 22 changes into the data of serial form the data of the parallel form supplied from LSI23 for attestation, and supplies it to the interface 16.

[0051]LSI23 for attestation supplies the digest and random number which were obtained from ASIC etc. by becoming and performing calculation of a digest, and generating of a random number according to the processing mentioned later to the game machine 1. LSI23 for attestation memorizes beforehand the substantially same common restricted data as what LSI17 for attestation of the game machine 1 has memorized. The above-mentioned digest (namely, data which serves as above-mentioned information on (6) by enciphering with the secret key for a signature) used for creation of signature data is memorized beforehand. (In addition, below, LSI23 for attestation calls the digest dA the above-mentioned digest memorized beforehand.)

[0052]The output unit 3 reproduces the sound which consisted of television receivers etc., and displayed the picture according to directions of the control section 11 of the game machine 1, and followed directions of the control section 11.

[0053](Operation) Next, operation of this game system is explained with reference to drawing 3 – drawing 5. Drawing 3 is a flow chart showing processing of a digital signature check. Drawing 4 is a flow chart showing processing of mutual recognition. Drawing 5 is a flow chart showing the procedure of execution of a game program.

[0054](Digital signature check) If the game machine 1 is started after the slot 15 is equipped with the cassette 2, and a user directs the start of a game using the input part 14, the game machine 1 will answer these directions and will perform first processing of the digital signature check shown in drawing 3.

[0055]If processing of a digital signature check is started, the control section 11 of the game machine 1 will access ROM21 of the cassette 2 via the interfaces 16 and 22. And the list for a signature (namely, above-mentioned information on (5)) stored in ROM21 and the signature data matched with the list for a signature concerned are read, and LSI17 for attestation is supplied (drawing 3, Step S101).

[0056]If the list for a signature and signature data are supplied from the control section 11 to LSI17 for attestation, The value assigned to the substantially same hash function as what was used in order to create the signature data stored in ROM21 in the data made into the object of encryption for creation of signature data. It calculates (this value is hereafter called digest dB), and digest dB is supplied to the control section 11 (Step S102).

[0057]The data made into the object of encryption for creation of signature data is the whole data specifically stored in the storage area which the list for a signature expresses as mentioned above. And in Step S102, LSI17 for attestation combines each data of each other which is in the storage area which the list for a signature expresses, for example in accordance with a predetermined rule, and calculates digest dB per [which created and created one data] data.

[0058]Next, LSI17 for attestation decrypts the signature data supplied at Step S101 using the public key for signature verification which self memorizes, and stores in the main memory part 12 the data (decrypted signature data) generated as a result of decryption (Step S103).

[0059]It is distinguished whether digest dB supplied from LSI17 for attestation at Step S102 and the decrypted signature data of the control section 11 which LSI17 for attestation generated at Step S103, and was stored in the main memory part 12 correspond substantially (Step S104). And if in agreement and it will distinguish, it points to the display of the picture which expresses failure in attestation with the output unit 3, and processing is ended, and the output unit 3 will answer these directions and will display the picture showing failure in attestation.

[0060](Processing of mutual recognition) On the other hand, in Step S104, if digest dB and decrypted signature data are substantially in agreement and it will distinguish, the control section 11 will perform processing of the mutual recognition shown in drawing 4.

[0061]If processing of mutual recognition is started, the control section 11 directs the start of attestation to LSI17 for attestation. LSI17 for attestation answers these directions and is supplied to LSI23 for attestation of the cassette 2 via the interfaces 16 and 22 by using as challenge data the random number which generated and generated the random number (drawing 4, Step S201).

[0062]If challenge data are supplied from LSI17 for attestation to LSI23 for attestation, The challenge data, the common restricted data which self memorizes, and self combine mutually three persons of the digest dA (digest which will serve as signature data if enciphered with the secret key for a signature) who memorize beforehand with a predetermined technique, and create one data (drawing 4, Step S301).

[0063]And the value (this value is hereafter called the digest dC) which substituted the created data for the predetermined hash function (for example, the substantially same hash function as what was used at Step S102) is calculated (Step S302). If the digest dC is computed at Step S302, LSI23 for attestation will be supplied to LSI17 for attestation of the game machine 1 via the interfaces 22 and 16 by using the digest dC as response data (Step S303).

[0064]If response data is supplied from LSI23 for attestation of the cassette 2 to LSI17 for attestation, Three persons of the challenge data which self supplied at Step S201, the common restricted data which self memorizes, and the decrypted signature data stored in the main memory part 12 in Step S103 of processing of a signature check are combined mutually, and one

data is created (Step S202).

[0065]And LSI17 for attestation calculates the digest (it is hereafter called the digest dD) of the data created at Step S202 using the substantially same hash function as what was used at Step S302 (Step S203). And the obtained digest dD distinguishes whether it is substantially the same as that of the response data (namely, digest dC) supplied to self at Step S303 (Step S204).

[0066]In Step S204, if the digest dD and response data distinguish substantially that it is the same, LSI17 for attestation will send the success message of a predetermined form to LSI23 for attestation of the cassette 2 (Step S205). If a success message is supplied to LSI23 for attestation from LSI17 for attestation of the game machine 1, it will answer this success message and will be supplied to LSI17 for attestation by using as challenge data the random number which generated and generated the random number (Step S304).

[0067]On the other hand, in Step S204, if in agreement and it will distinguish, LSI17 for attestation will notify failure in attestation to the control section 11 of the game machine 1. The control section 11 points to the display of the picture showing failure in attestation to the output unit 3, ends processing, and the output unit 3 answers these directions and it displays the picture showing failure in attestation.

[0068]If challenge data are supplied from LSI23 for attestation at Step S304 to LSI17 for attestation, Three persons of the challenge data, the common restricted data which self memorizes, and the decrypted signature data stored in the main memory part 12 at Step S103 are mutually combined with a predetermined technique, and one data is created (Step S206).

[0069]And the digest (digest dE) of the data created at Step S206, LSI23 for attestation of the cassette 2 is supplied by using as response data the digest dE obtained by calculating using the substantially same hash function as what was used at Step S302 (Step S207).

[0070]If response data is supplied from the game machine 1 at Step S207 to LSI23 for attestation, The challenge data, common restricted data, and self which self supplied at Step S304 combine mutually three persons of a digest who memorize beforehand, and create one data (Step S305).

[0071]And LSI23 for attestation calculates the digest (digest dF) of the data created at Step S305 using the substantially same hash function as what was used at Step S302 (Step S306). And the obtained digest dF distinguishes whether it is substantially in agreement with the response data (namely, digest dE) supplied to self at Step S207 (Step S307).

[0072]In Step S307, if in agreement and it will distinguish, LSI17 for attestation will notify failure in attestation to the control section 11. The control section 11 points to the display of the picture showing failure in attestation to the output unit 3, ends processing, and the output unit 3 answers these directions and it displays the picture showing failure in attestation.

[0073]On the other hand, in Step S307, if the digest dF and response data are substantially in agreement and it will distinguish, LSI23 for attestation will send the success message of a predetermined form to LSI17 for attestation of the game machine 1 (Step S308), and will end processing of mutual recognition. LSI17 for attestation to which the success message was supplied at Step S308 notifies a success of attestation to the control section 11 (Step S208), and ends processing of mutual recognition.

[0074](Execution of a game program) If the notice of a success of attestation is supplied to the control section 11, this game system will execute a game program succeedingly in the procedure shown in drawing 5.

[0075]First, the control section 11 reads an encryption encryption key from ROM21, and supplies it to LSI17 for attestation. LSI17 for attestation decrypts an encryption encryption key using the secret key for key decryption which self memorizes, and supplies the encryption key obtained by decryption to the control section 11 (drawing 5, Step S401). The control section 11 to which the encryption key was supplied reads an encryption position list from ROM21 (Step S402).

[0076]Next, the control section 11 specifies and reads what expresses processing of the beginning of a game program among the data stored in ROM21 (Step S403). The header of a predetermined form is beforehand given to the data which may perform specification of the first processing by arbitrary techniques, for example, expresses the first processing, and the control section 11 should just retrieve the header concerned from the inside of the data stored in

ROM21.

[0077]Next, the control section 11 distinguishes whether the data read at Step S403 is an encryption module by analyzing the contents of the encryption position list read at Step S402 (Step S404). And if it is not an encryption module, processing which the non-enciphering module concerned expresses will be performed (Step S405). (if it is a non-enciphering module) If it is an encryption module, the encryption module concerned will be decrypted using the encryption key supplied to self at Step S401 (Step S406), and processing which the data obtained by decryption expresses will be performed (Step S407).

[0078]And in the processing performed by Step S405 or S407, if other processings are called, the control section 11 will read the data showing the called processing, will treat the data as data specified at Step S403, and will move processing to Step S404.

[0079]That is, the control section 11 distinguishes whether the data which read the data showing the processing called by Step S405 or S407, and was read based on the contents of the encryption position list is an encryption module. And if it is not an encryption module, processing will be moved to Step S405, and if it is an encryption module, processing will be moved to Step S406.

[0080]By processing explained above, this game system executes a game program according to the data stored in ROM21. When the data which expresses processing of the object which should be performed in that case is enciphered, the processing concerned is performed after decrypting the data.

[0081]As explained above, in this game system. If it is not necessary to set the whole game program of the object to perform as the object of a signature for example, and a part of game program is used for signature data creation, the purpose of protecting the game program concerned from unjust access will be attained substantially.

[0082]And it is if a part of game program is made into the object of a signature (.) as mentioned above. That is, if a vermin type is signed, as a result of calculation of a digest becoming high-speed compared with the case where the whole game program is set as the object of a signature, processing of a signature check becomes high-speed and a smooth advance of a game becomes is hard to be checked.

[0083]If the data which does not need to encipher the whole game program of the object to perform, for example, expresses processing of an important scene with this game system on advance of a game is enciphered, the purpose of protecting the game program concerned from unjust access will be attained substantially.

[0084]And as mentioned above, if a game program is enciphered selectively (at vermin type), compared with the case where the whole game program is enciphered, execution of a game program will become high-speed and a smooth advance of a game will become is hard to be checked. As a result of the abbreviation of encryption, the information-redundancy nature stored in ROM21 becomes small, and storing of the data of ROM21 becomes efficient.

[0085]The composition of this game system is not restricted to an above-mentioned thing. For example, the data which ROM21 memorizes does not need to express the program of the game which the game machine 1 performs, and the game machine 1 does not need to be a device for executing a game program, either. The cassette 2 does not need to store in ROM21 the data of the object supplied to the game machine 1, and the data of the object supplied to the game machine 1 may be stored in CD-ROM, DVD (Digital Video Disk), and other arbitrary recording media, for example. The game machine 1 and the cassette 2 of each other do not need to be connected removable, it may be connected fixed mutually and both may exchange data mutually via a communication line.

[0086]The control section 11 may function LSI17 for attestation, two or more integrated circuits may be made to function about LSI17 for attestation, and two or more integrated circuits may be made to function about LSI23 for attestation. The game machine 1 may memorize beforehand the encryption key used for decryption of data at Step S406.

[0087]The storage area which LSI23 for attestation of the cassette 2 has and which memorizes the digest dA may be a storage area which the nonvolatile storage in which 1-time writing, such as PROM (Programmable Read Only Memory), is possible has, for example. In this case, it is not

necessary to manufacture LSI23 for attestation individually every cassette 2 by which the data stored in ROM21 differs. Therefore, LSI23 for attestation in the state where the contents of the storage area which can be written in were initialized once for example, is mass-produced, and it may be made to write the digest dA in the storage area in which the 1-time writing of each LSI23 for attestation is possible after that.

[0088]The storage area which memorizes the secret key for key encryption which LSI17 for attestation of the game machine 1 has, and the public key for signature verification, It may be a storage area which the rewritable nonvolatile storage of EEPROM (Electrically Erasable/Programable Read Only Memory) etc. has. In this case, LSI17 for attestation may mass-produce LSI17 for attestation in the state where the data acquired from the cassette 2 differs and where did not need to manufacture individually for every thing, for example, the contents of the rewritable storage area were initialized. And the user etc. of the game machine 1 provided with LSI17 for attestation by which the contents of the rewritable storage area were initialized, It may be made to write the public key required in order to attest the cassette 2 which is due to be connected to the game machine 1 for signature verification, etc. in the storage area which can rewrite LSI17 for attestation of the game machine 1.

[0089]ROM21 matches with an encryption module and it may be made to store the signature data for encryption modules with above-mentioned separate signature data. The signature data for encryption modules should just encipher the encryption module matched with self using the 3rd secret key separate from the secret key for an above-mentioned signature, or the secret key for key decryption, for example. In this case, LSI17 for attestation should just memorize beforehand the 3rd secret key concerned and the 3rd public key that makes a pair, for example.

[0090]Thereby, the privacy of an encryption module improves further. The inside of the program data of the game program stored in ROM21 of the cassette 2, for example, It becomes applicable [** which sets except the portion showing processing of the game of the trial version as the object of a signature individually, and enables it to perform the game of the trial version using the game machine 1 which has not memorized the 3rd public key].

[0091]When the signature data for encryption modules is matched with the encryption module, this game system should just execute a game program in the procedure shown in drawing 6, after the notice of a success of attestation is supplied to the control section 11. In the procedure shown in drawing 6, the processing which attached the same reference number as what is shown in drawing 5 expresses the substantially same processing as what is shown in drawing 5.

[0092]That is, if the notice of a success of attestation is supplied to the control section 11, this game system will perform the same processing substantially with Steps S401-S404 of drawing 5 successively (drawing 6, Steps S401-S404). In processing (the processing as Step 404 got blocked that drawing 5 is substantially the same) of Step 404 of drawing 6, When it distinguishes that the data specified at Step S403 is an encryption module, it is distinguished whether the control section 11 has the signature data for encryption modules matched with the data (Step S408).

[0093]And when there was nothing and it distinguishes, the control section 11 moves processing to Step S406. When it was and distinguishes, the applicable signature data for encryption modules is read, and the read signature data for encryption modules and the encryption module read at Step S403 are supplied to LSI17 for attestation (Step S409).

[0094]LSI17 for attestation the encryption module supplied from the control section 11, A predetermined hash function (for example, the value (it is hereafter called the digest dG) assigned to the substantially same hash function as what was used at Step S102 is calculated, and the digest dG is supplied to the control section 11 (Step S410).)

[0095]Next, LSI17 for attestation decrypts the signature data for encryption modules supplied at Step S409 using the 3rd public key that self memorizes, and supplies the data obtained by decryption to the control section 11 (Step S411).

[0096]Next, it is distinguished whether the digest dG supplied from LSI17 for attestation at Step S410 and the data of the control section 11 supplied from LSI17 for attestation at Step S411 correspond substantially (Step S412). And if in agreement and it will distinguish, and processing is moved to Step S406, it is not in agreement and it will distinguish, it points to the display of the

picture which expresses failure in attestation with the output unit 3, and execution of a game program is ended, and the output unit 3 will answer these directions and will display the picture showing failure in attestation.

[0097]A digital signature may be given to encryption position data using the secret key separate from the secret key for an above-mentioned signature for encryption position data. In this case, the information which shows the storage area which does not need to use encryption position data for creation of signature data (namely, above-mentioned information on (6)) therefore, where encryption position data is stored in the list for a signature does not need to be included.

[0098]When encryption position data is given the digital signature using the secret key for encryption position data, LSI17 for attestation of the game machine 1 may memorize the secret key for encryption position data, and the public key for encryption position data attestation which makes a pair, for example. And before the game machine 1 shifts to processing of Step S403, it may be made to attest that use the public key for encryption position data attestation, and encryption position data is created by the regular supply origin of the cassette 2, for example after processing of the above-mentioned step S402.

[0099]As mentioned above, although this embodiment of the invention was described, the authentication system and authentication device of this invention cannot be based on a system for exclusive use, but can be realized using the usual computer system. For example, the authentication device and authentication system which perform above-mentioned processing can be constituted by installing this program from the media (a floppy disk, CD-ROM, etc.) which stored the program for performing above-mentioned operation in the personal computer.

[0100]Communication media (medium which holds a program temporarily and fluidly like a communication line, a communication network, and a communications system) may be sufficient as the medium for supplying a program to a computer. For example, this program may be put up for the bulletin board (BBS) of a communication network, and this may be distributed via a network. And above-mentioned processing can be performed by starting this program and performing like other application programs under control of OS.

[0101]When OS shares a part of processing, or when OS constitutes a part of one component of the invention in this application, the program except the portion may be stored in a recording medium. Also in this case, the program for performing each function or step which a computer performs shall be stored in that recording medium by this invention.

[0102]

[Effect of the Invention]As explained above, according to this invention, supply of the game machine by a regular supplier and a cartridge is secured, and the authentication system and authentication device with which read-out of data and the duplicate of a cartridge are prevented are realized.

[Translation done.]

*** NOTICES ***

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a block diagram showing the basic constitution of the game system concerning this embodiment of the invention.

[Drawing 2]It is a figure showing typically the data structure of the data stored in ROM.

[Drawing 3]It is a flow chart showing processing of a digital signature check.

[Drawing 4]It is a flow chart showing processing of mutual recognition.

[Drawing 5]It is a flow chart showing the procedure of execution of a game program.

[Drawing 6]It is a flow chart showing the modification of the procedure of execution of a game program.

[Description of Notations]

1 Game machine

11 Control section

12 Main memory part

13 External memory part

14 Input part

15 Slot

16 and 22 Interface

17 and 23 LSI for attestation

2 Cassette

21 ROM

[Translation done.]

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-76063

(P2000-76063A)

(43)公開日 平成12年3月14日 (2000.3.14)

(51) Int.Cl. ⁷ G 0 6 F 9/06 A 6 3 F 13/00 G 0 6 F 12/14	識別記号 5 5 0 3 2 0	F I G 0 6 F 9/06 A 6 3 F 9/22 G 0 6 F 12/14	5 5 0 H 2 C 0 0 1 5 5 0 A 5 B 0 1 7 A 5 B 0 7 6 3 2 0 A	テーマコード(参考) 2 C 0 0 1 5 B 0 1 7 A 5 B 0 7 6 3 2 0 A
---	------------------------	--	--	--

審査請求 未請求 請求項の数18 O.L (全 18 頁)

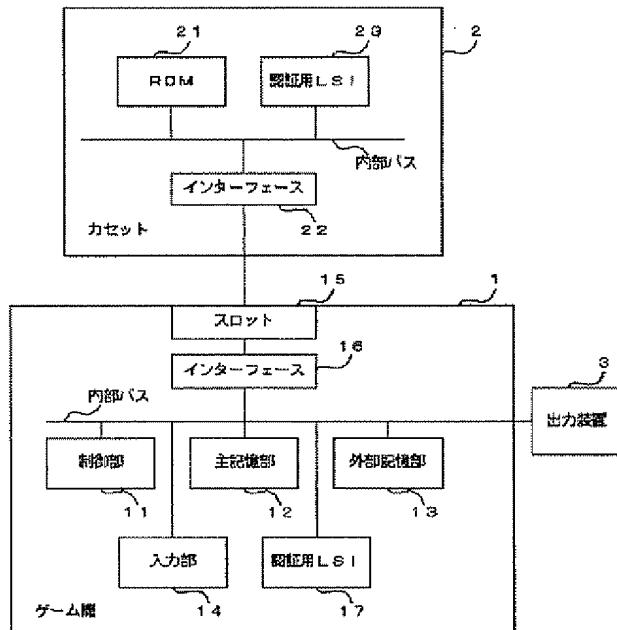
(21) 出願番号 特願平10-244762	(71) 出願人 株式会社オープンループ 北海道札幌市清田区清田七条一丁目18番5号
(22) 出願日 平成10年8月31日 (1998.8.31)	(72) 発明者 浅田 一憲 北海道札幌市清田区北野七条二丁目5番5号 株式会社オープンループ内
	(74) 代理人 100095407 弁理士 木村 满 (外2名)
	F ターム(参考) 2C001 AA00 AA17 BD00 BD04 BD07 CB01 CB03 CB05 5B017 AA03 AA06 BA07 BA09 BB06 5B076 FA13 FB07 FB12

(54) 【発明の名称】 認証システム、認証装置及び記録媒体

(57) 【要約】

【課題】 正規の供給者によるゲーム機及びカートリッジの供給が確保され、データの読み出しやカートリッジの複製が阻止される認証システム等を提供する。

【解決手段】 ゲーム機1は、カセット2のデータと、そのデータのダイジェストを暗号化した署名データを読み込み、読み込んだデータのダイジェストと復号化した署名データとを比較し、カセット2を認証する。次に、カセット2は、ゲーム機1が供給したチャレンジデータ、自ら記憶するダイジェスト及び共通秘密データの三者のダイジェストをレスポンスデータとしてゲーム機1に返す。ゲーム機1は、そのレスポンスデータが、チャレンジデータ、復号化した署名データ及び自ら記憶する共通秘密データの三者のダイジェストと一致するか否かを判別し、カセット2を認証する。同様にカセット2もゲーム機1を認証し、その後、ゲーム機1はカセット2が記憶するプログラムを実行する。



【特許請求の範囲】

【請求項1】本体側認証部と、カートリッジ側認証部と、を備え、

前記本体側認証部は、

自己に固有の本体側署名データを記憶する本体側記憶手段と、

前記カートリッジ側認証部からカートリッジ側署名データを取得して、そのカートリッジ側署名データが前記カートリッジ側認証部に固有のものであるか否かを判別し、固有のものであると判別したとき、前記カートリッジ側認証部から転送対象データを取得する本体側判別手段と、を備え、

前記カートリッジ側認証部は、
前記転送対象データを記憶する記憶手段と、

前記カートリッジ側署名データを記憶するカートリッジ側記憶手段と、

前記本体側認証部から前記本体側署名データを取得して、その本体側署名データが前記本体側認証部に固有のものであるか否かを判別し、固有のものであると判別したとき、前記記憶手段が記憶している前記転送対象データを前記本体側認証部に供給するカートリッジ側判別手段と、を備える、

ことを特徴とする認証システム。

【請求項2】前記カートリッジ側署名データは、特定のデータを所定の一方向性関数に代入した値を表すダイジェストを秘密鍵を用いて暗号化したものを表しており、前記カートリッジ側記憶手段は、前記特定のデータを記憶する手段を備え、

前記本体側認証部は、前記カートリッジ側認証部から前記特定のデータを取得し、前記カートリッジ側署名データを公開鍵を用いて復号化し、復号化された前記カートリッジ側署名データが前記ダイジェストと実質的に同一のものであるか否かを判別して、実質的に同一のものであると判別したとき、前記カートリッジ側署名データが前記カートリッジ側認証部に固有のものであるか否かを判別する、

ことを特徴とする請求項1に記載の認証システム。

【請求項3】前記特定のデータは、前記転送対象データのうち予め特定された部分からなり、

前記カートリッジ側記憶手段は、前記部分を特定する署名対象識別データを記憶する手段を備え、

前記本体側認証部は、前記カートリッジ側記憶手段より前記署名対象識別データを取得して、前記転送対象データのうち、取得した前記署名対象識別データにより特定される前記部分を、前記特定のデータとして取得する手段を備える、

ことを特徴とする請求項2に記載の認証システム。

【請求項4】前記署名対象識別データにより特定される前記部分は、前記本体側認証部が前記特定のデータを取得してから復号化された前記カートリッジ側署名データ

が前記ダイジェストと実質的に同一のものであるか否かを判別するまでの所要時間が一定時間以内となるように選ばれている、

ことを特徴とする請求項3に記載の認証システム。

【請求項5】前記本体側認証部は、外部から供給された前記公開鍵を書き換え可能に記憶する鍵記憶手段を備え、前記カートリッジ側署名データを、前記鍵記憶手段が記憶する前記公開鍵を用いて復号化する、
ことを特徴とする請求項2、3又は4に記載の認証システム。

【請求項6】前記本体側記憶手段及び前記カートリッジ側記憶手段は、それぞれ、互いに実質的に同一の共通秘密データを記憶する手段を備え、

前記本体側判別手段は、

本体側チャレンジデータを作成して前記カートリッジ側判別手段に供給する手段と、

前記カートリッジ側判別手段よりカートリッジ側チャレンジデータを取得し、取得したカートリッジ側チャレンジデータ、復号化された前記カートリッジ側署名データ及び前記本体側記憶手段が記憶する前記共通秘密データの三者を表すデータを前記一方向性関数に代入した値を表す本体側レスポンスデータを作成して前記カートリッジ側判別手段に供給する手段と、

前記カートリッジ側判別手段よりカートリッジ側レスポンスデータを取得し、前記本体側チャレンジデータ、復号化された前記カートリッジ側署名データ及び前記本体側記憶手段が記憶する前記共通秘密データの三者を表すデータを前記一方向性関数に代入した値が前記カートリッジ側レスポンスデータを表すか否かを判別して、表すと判別したとき、前記カートリッジ側署名データが前記カートリッジ側認証部に固有のものであると判別する手段を備え、

前記カートリッジ側記憶手段は、前記ダイジェストを記憶するダイジェスト記憶手段を備え、

前記カートリッジ側判別手段は、

前記カートリッジ側チャレンジデータを作成して前記本体側判別手段に供給する手段と、

前記本体側判別手段より前記本体側チャレンジデータを取得し、取得した前記本体側チャレンジデータ、前記カートリッジ側記憶手段が記憶する前記ダイジェスト及び前記カートリッジ側記憶手段が記憶する前記共通秘密データの三者を表すデータを前記一方向性関数に代入した値を表す前記カートリッジ側レスポンスデータを作成して前記本体側判別手段に供給する手段と、

前記本体側判別手段より前記本体側レスポンスデータを取得し、前記カートリッジ側チャレンジデータ、前記カートリッジ側記憶手段が記憶する前記ダイジェスト及び前記カートリッジ側記憶手段が記憶する前記共通秘密データの三者を表すデータを前記一方向性関数に代入した値が前記本体側レスポンスデータを表すか否かを判別し

て、表すと判別したとき、前記本体側署名データが前記本体側認証部に固有のものであると判別する手段を備える、ことを特徴とする請求項2乃至5のいずれか1項に記載の認証システム。

【請求項7】前記ダイジェスト記憶手段は、外部から供給される前記ダイジェストを実質的に不揮発的に記憶する手段を備える、

ことを特徴とする請求項6に記載の認証システム。

【請求項8】前記記憶手段は、暗号化済みの前記転送対象データを記憶する手段を備え、

前記本体側認証部は、前記カートリッジ側認証部から取得したカートリッジ側署名データが前記カートリッジ側認証部に固有のものであると判別したとき、暗号化済みの前記転送対象データを前記カートリッジ側認証部から取得して復号化する手段を備える、

ことを特徴とする請求項2乃至7のいずれか1項に記載の認証システム。

【請求項9】前記記憶手段は、暗号化済みの前記転送対象データを、暗号化された当該転送対象データに固有の暗号化データ用署名データと対応付けて記憶する手段を備え、

前記本体側認証部は、前記カートリッジ側認証部から取得したカートリッジ側署名データが前記カートリッジ側認証部に固有のものであると判別したとき、前記カートリッジ側認証部から前記暗号化データ用署名データを取得し、

取得した前記暗号化データ用署名データが、当該暗号化データ用署名データに対応付けられた暗号化済みの前記転送対象データに固有のものであるか否かを判別して、固有的ものであると判別したとき、当該暗号化データ用署名データに対応付けられた暗号化済みの前記転送対象データを取得して復号化する手段を備える、

ことを特徴とする請求項8に記載の認証システム。

【請求項10】前記記憶手段は、自己が有する記憶領域のうち暗号化済みの前記転送対象データを記憶する部分の論理的位置を識別する位置データを記憶する手段を備え、

前記特定のデータは当該位置データを含んでおり、前記本体側認証部は、前記記憶手段が有する記憶領域のうち前記位置データにより識別される論理的位置から暗号化済みの前記転送対象データを取得して復号化する手段を備える、

ことを特徴とする請求項8又は9に記載の認証システム。

【請求項11】前記記憶手段は、自己が有する記憶領域のうち暗号化済みの前記転送対象データを記憶する部分の論理的位置を識別する位置データを記憶する手段と、

前記位置データに固有の位置データ用署名データを記憶

する手段と、を備え、

前記本体側認証部は、前記カートリッジ側認証部から前記位置データ用署名データを取得し、取得した前記位置データ用署名データが前記位置データに固有のものであるか否かを判別して、固有的ものであると判別したとき、前記記憶手段が有する記憶領域のうち前記位置データにより識別される論理的位置から暗号化済みの前記転送対象データを取得して復号化する手段を備える、

ことを特徴とする請求項8又は9に記載の認証システム。

【請求項12】転送対象データを記憶する記憶手段と、特定のデータ、及び当該特定のデータを所定の一方向性関数に代入した値を表すダイジェストを秘密鍵を用いて暗号化したものと表すカートリッジ側署名データを記憶するカートリッジ側記憶手段と、自己に接続された装置から本体側署名データを取得して、その本体側署名データが当該装置に固有のものであるか否かを判別し、固有的ものであると判別したとき、前記記憶手段が記憶している前記転送対象データを当該装置に供給するカートリッジ側判別手段と、を備えるカートリッジ側認証装置に着脱可能に接続される認証装置であって、

自己に固有の前記本体側署名データを記憶する本体側記憶手段と、

前記カートリッジ側認証装置から前記特定のデータを取得し、前記カートリッジ側署名データを公開鍵を用いて復号化し、復号化された前記カートリッジ側署名データが前記ダイジェストと実質的に同一のものであるか否かを判別して、実質的に同一のものであると判別したとき、前記カートリッジ側認証装置から前記転送対象データを取得する本体側判別手段と、を備える、

ことを特徴とする認証装置。

【請求項13】自己に固有の本体側署名データを記憶する本体側記憶手段と、

特定のデータ、及び当該特定のデータを所定の一方向性関数に代入した値を表すダイジェストを秘密鍵を用いて暗号化したものと表すカートリッジ側署名データとを記憶する装置から前記カートリッジ側署名データ及び前記特定のデータを取得して、取得した前記カートリッジ側署名データを公開鍵を用いて復号化し、復号化された前記カートリッジ側署名データが前記ダイジェストと実質的に同一のものであるか否かを判別して、実質的に同一のものであると判別したとき、前記装置から転送対象データを取得する本体側判別手段と、を備える本体側認証装置に着脱可能に接続される認証装置であって、

前記転送対象データを記憶する記憶手段と、

前記カートリッジ側署名データ及び前記特定のデータを記憶するカートリッジ側記憶手段と、

前記本体側認証装置から前記本体側署名データを取得して、その本体側署名データが前記本体側認証装置に固有のものであるか否かを判別し、固有的ものであると判別

したとき、前記記憶手段が記憶している前記転送対象データを前記本体側認証装置に供給するカートリッジ側判別手段と、を備える、
ことを特徴とする認証装置。

【請求項14】第1及び第2の認証部を備え、
前記第1の認証部は、

自己に固有の第1の署名データを記憶する第1の記憶手段と、

前記第2の認証部から特定のデータを取得し、第2の署名データを公開鍵を用いて復号化し、復号化された前記第2の署名データが、特定のデータを所定の一方向性関数に代入した値を表すダイジェストと実質的に同一のものであるか否かを判別して、実質的に同一のものであると判別したとき、前記第2の署名データが前記第2の認証部に固有のものであるか否かを判別し、固有のものであると判別したとき、前記第2の認証部から転送対象データを取得する第1の判別手段と、を備え、

前記第2の認証部は、

前記転送対象データ及び前記第2の署名データを記憶する第2の記憶手段と、

前記第1の認証部から前記第1の署名データを取得して、その第1の署名データが前記第1の認証部に固有のものであるか否かを判別し、固有のものであると判別したとき、前記第2の記憶手段が記憶している前記転送対象データを前記第1の認証部に供給する第2の判別手段と、を備え、

前記第2の署名データは、前記転送対象データのうちの予め特定された部分を表す前記特定のデータを所定の一方向性関数に代入した値を秘密鍵を用いて暗号化したものを表す、

ことを特徴とする認証システム。

【請求項15】前記第2の記憶手段は、暗号化済みの前記転送対象データを記憶する手段を備え、

前記第1の認証部は、前記第2の認証部から取得した第2の署名データが前記第2の認証部に固有のものであると判別したとき、暗号化済みの前記転送対象データを前記第2の認証部から取得して復号化する手段を備える、
ことを特徴とする請求項14に記載の認証システム。

【請求項16】前記第2の記憶手段は、暗号化済みの前記転送対象データを、暗号化された当該転送対象データに固有の暗号化データ用署名データと対応付けて記憶する手段を備え、

前記第1の認証部は、前記第2の認証部から取得した第2の署名データが前記第2の認証部に固有のものであると判別したとき、前記第2の認証部から前記暗号化データ用署名データを取得し、取得した前記暗号化データ用署名データが、当該暗号化データ用署名データに対応付けられた暗号化済みの前記転送対象データに固有のものであるか否かを判別して、固有のものであると判別したとき、当該暗号化データ用署名データに対応付けられた

暗号化済みの前記転送対象データを取得して復号化する手段を備える、

ことを特徴とする請求項15に記載の認証システム。

【請求項17】転送対象データを記憶する記憶手段と、特定のデータ、及び当該特定のデータを所定の一方向性関数に代入した値を表すダイジェストを秘密鍵を用いて暗号化したものを表すカートリッジ側署名データを記憶するカートリッジ側記憶手段と、自己に接続された装置から本体側署名データを取得して、その本体側署名データが当該装置に固有のものであるか否かを判別し、固有のものであると判別したとき、前記記憶手段が記憶している前記転送対象データを当該装置に供給するカートリッジ側判別手段と、を備えるカートリッジ側認証装置に着脱可能に接続されたコンピュータを、

自己に固有の前記本体側署名データを記憶する本体側記憶手段と、

前記カートリッジ側認証装置から前記特定のデータを取得し、前記カートリッジ側署名データを公開鍵を用いて復号化し、復号化された前記カートリッジ側署名データ

20 が前記ダイジェストと実質的に同一のものであるか否かを判別して、実質的に同一のものであると判別したとき、前記カートリッジ側認証装置から前記転送対象データを取得する本体側判別手段と、
して機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項18】自己に固有の本体側署名データを記憶する本体側記憶手段と、

特定のデータ、及び当該特定のデータを所定の一方向性関数に代入した値を表すダイジェストを秘密鍵を用いて暗号化したものを表すカートリッジ側署名データを記憶する装置から前記カートリッジ側署名データ及び前記特定のデータを取得して、取得した前記カートリッジ側署名データを公開鍵を用いて復号化し、復号化された前記カートリッジ側署名データが前記ダイジェストと実質的に同一のものであるか否かを判別して、実質的に同一のものであると判別したとき、前記装置から転送対象データを取得する本体側判別手段と、を備える本体側認証装置に着脱可能に接続されたコンピュータを、

前記転送対象データを記憶する記憶手段と、

40 前記カートリッジ側署名データ及び前記特定のデータを記憶するカートリッジ側記憶手段と、

前記本体側認証装置から前記本体側署名データを取得して、その本体側署名データが前記本体側認証装置に固有のものであるか否かを判別し、固有のものであると判別したとき、前記記憶手段が記憶している前記転送対象データを前記本体側認証装置に供給するカートリッジ側判別手段と、
して機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、認証システム及び認証装置に関し、特に、データの利用者や供給者を制限するための認証システム及び認証装置に関する。

【0002】

【従来の技術】ゲーム機がユーザにゲームを提供する場合は、通常、ゲームプログラムを格納したROM(Read Only Memory)等の記憶装置を含むカートリッジがゲーム機に装着され、ゲーム機はカートリッジの記憶装置からゲームプログラムのプログラムデータを読み出し、そのゲームプログラムを実行するようにしていた。

【0003】

【発明が解決しようとする課題】しかし、消費者保護のため市場に供給されるゲームの質を維持する等の目的で、ゲームの供給者を一定の範囲の者に制限する場合は、ゲーム供給の許可を得ていない者によりゲームが供給されることを防止する必要がある。ところが、上述の手法では、無許可でのゲームの供給を阻止することができない。

【0004】上述の事情はゲーム機本体についても同様である。すなわち、ゲーム機の品質維持による消費者保護のため無許可でのゲーム機の供給を防止する必要がある場合であっても、上述の手法では、無許可でのゲーム機の供給を阻止することができない。

【0005】また、正規のゲーム供給者により供給されたカートリッジであっても、そのカートリッジが不正に複製されることにより、正規に購入されたものでないカートリッジが流通する危険があり、上述の手法では、カートリッジの不正な複製を阻止することができない。

【0006】また、カートリッジ全体の複製に至らなくても、カートリッジの記憶装置に格納されているデータが不正に読み出されて解析される等の危険はある。そして、不正に読み出されたデータが記憶装置に格納された上で、その記憶装置がカートリッジに組み込まれれば、結局、共通のカートリッジを用いて複数のゲームが不正に行われるようになってしまう。

【0007】さらに、読み出されたデータが単独で商品価値を有する場合（例えば、そのデータが画像データである場合）などは、そのデータからゲームを再現することができない場合であっても、そのデータが単独で流通してしまう危険が大きい。

【0008】この発明は上記実状に鑑みてなされたもので、正規の供給者によるゲーム機及びカートリッジの供給が確保され、データの読み出しやカートリッジの複製が阻止される認証システム及び認証装置を提供することを目的とする。

【0009】

【課題を解決するための手段】上記目的を達成するため、この発明の第1の観点にかかる認証システムは、本体側認証部と、カートリッジ側認証部と、を備え、前記

10

20

30

40

50

本体側認証部は、自己に固有の本体側署名データを記憶する本体側記憶手段と、前記カートリッジ側認証部からカートリッジ側署名データを取得して、そのカートリッジ側署名データが前記カートリッジ側認証部に固有のものであるか否かを判別し、固有のものであると判別したとき、前記カートリッジ側認証部から転送対象データを取得する本体側判別手段と、を備え、前記カートリッジ側認証部は、前記転送対象データを記憶する記憶手段と、前記カートリッジ側署名データを記憶するカートリッジ側記憶手段と、前記本体側認証部から前記本体側署名データを取得して、その本体側署名データが前記本体側認証部に固有のものであるか否かを判別し、固有のものであると判別したとき、前記記憶手段が記憶している前記転送対象データを前記本体側認証部に供給するカートリッジ側判別手段と、を備える、ことを特徴とする。

【0010】このような認証システムによれば、本体側認証部とカートリッジ側認証部は、互いが正規に製造されたものであることを認証した上で、転送対象データの送受を行なう。従って、カートリッジ側署名データの作成や秘密鍵の入手を許されていない者から転送対象データが供給されることが阻止される。

【0011】前記カートリッジ側署名データは、例えば、特定のデータを所定の一方向性関数に代入した値を表すダイジェストを秘密鍵を用いて暗号化したものを表しており、この場合、前記カートリッジ側記憶手段は、前記特定のデータを記憶する手段を備え、前記本体側認証部は、前記カートリッジ側認証部から前記特定のデータを取得し、前記カートリッジ側署名データを公開鍵を用いて復号化し、復号化された前記カートリッジ側署名データが前記ダイジェストと実質的に同一のものであるか否かを判別して、実質的に同一のものであると判別したとき、前記カートリッジ側署名データが前記カートリッジ側認証部に固有のものであるか否かを判別するものであってもよい。これにより、本体側認証部はまず、カートリッジ側署名データの正当性を検証するので、転送対象データの不正な供給の危険は更に減少する。

【0012】前記特定のデータは、前記転送対象データのうち予め特定された部分からなり、前記カートリッジ側記憶手段は、前記部分を特定する署名対象識別データを記憶する手段を備え、前記本体側認証部は、前記カートリッジ側記憶手段より前記署名対象識別データを取得して、前記転送対象データのうち、取得した前記署名対象識別データにより特定される前記部分を、前記特定のデータとして取得する手段を備えるものであってもよい。そして、例えば、前記署名対象識別データにより特定される前記部分は、前記本体側認証部が前記特定のデータを取得してから復号化された前記カートリッジ側署名データが前記ダイジェストと実質的に同一のものであるか否かを判別するまでの所要時間が一定時間以内となるように選ばれているものとしてもよい。これにより、

本体側認証部がカートリッジ側署名データとダイジェストとの同一性を確認するために要する時間が短く抑えられ、転送対象データの転送が円滑に行われる。

【0013】前記本体側認証部は、外部から供給された前記公開鍵を書き換え可能に記憶する鍵記憶手段を備え、前記カートリッジ側署名データを、前記鍵記憶手段が記憶する前記公開鍵を用いて復号化するものとすれば、本体側認証部は、個々のカートリッジ側認証部を認証するためのものとして個別に製造される必要はないこととなり、例えば、鍵記憶手段の記憶内容が初期化された状態で本体側認証部を量産し、後に鍵記憶手段に公開鍵を書き込めばよいこととなる。

【0014】前記本体側記憶手段及び前記カートリッジ側記憶手段は、例えば、それぞれ、互いに実質的に同一の共通秘密データを記憶する手段を備え、この場合、前記本体側判別手段は、例えば、本体側チャレンジデータを作成して前記カートリッジ側判別手段に供給する手段と、前記カートリッジ側判別手段よりカートリッジ側チャレンジデータを取得し、取得したカートリッジ側チャレンジデータ、復号化された前記カートリッジ側署名データ及び前記本体側記憶手段が記憶する前記共通秘密データの三者を表すデータを前記一方向性関数に代入した値を表す本体側レスポンスデータを作成して前記カートリッジ側判別手段に供給する手段と、前記カートリッジ側判別手段よりカートリッジ側レスポンスデータを取得し、前記本体側チャレンジデータ、復号化された前記カートリッジ側署名データ及び前記本体側記憶手段が記憶する前記共通秘密データの三者を表すデータを前記一方向性関数に代入した値が前記カートリッジ側レスポンスデータを表すか否かを判別して、表すと判別したとき、前記カートリッジ側署名データが前記カートリッジ側認証部に固有のものであると判別する手段を備えることにより、カートリッジ側認証部が正規に製造されたものであることを認証する。そして、前記カートリッジ側記憶手段は、前記ダイジェストを記憶するダイジェスト記憶手段を備え、前記カートリッジ側判別手段は、例えば、前記カートリッジ側チャレンジデータを作成して前記本体側判別手段に供給する手段と、前記本体側判別手段より前記本体側チャレンジデータを取得し、取得した前記本体側チャレンジデータ、前記カートリッジ側記憶手段が記憶する前記ダイジェスト及び前記カートリッジ側記憶手段が記憶する前記共通秘密データの三者を表すデータを前記一方向性関数に代入した値を表す前記カートリッジ側レスポンスデータを作成して前記本体側判別手段に供給する手段と、前記本体側判別手段より前記本体側レスポンスデータを取得し、前記カートリッジ側チャレンジデータ、前記カートリッジ側記憶手段が記憶する前記ダイジェスト及び前記カートリッジ側記憶手段が記憶する前記共通秘密データの三者を表すデータを前記一方向性関数に代入した値が前記本体側レスポンスデータを

表すか否かを判別して、表すと判別したとき、前記本体側署名データが前記本体側認証部に固有のものであると判別する手段を備えることにより、本体側認証部が正規に製造されたものであることを認証する。

【0015】また、前記ダイジェスト記憶手段は、外部から供給される前記ダイジェストを実質的に不揮発的に記憶する手段を備えるものとすれば、カートリッジ側認証部は、記憶する転送対象データが異なるもの毎に個別に製造される必要はないこととなり、例えば、ダイジェストを不揮発的に記憶する手段の記憶内容が初期化された状態でカートリッジ側認証部を量産し、後にカートリッジ側認証部にダイジェストを書き込めばよいこととなる。

【0016】前記記憶手段は、暗号化済みの前記転送対象データを記憶する手段を備え、前記本体側認証部は、前記カートリッジ側認証部から取得したカートリッジ側署名データが前記カートリッジ側認証部に固有のものであると判別したとき、暗号化済みの前記転送対象データを前記カートリッジ側認証部から取得して復号化する手段を備えるものであってもよい。

【0017】これにより、暗号化された転送対象データについては、その秘匿性が更に向上する。また、転送対象データのうち、当該データの利用価値に影響を及ぼす部分を虫食い式に暗号化するなどすれば、データの転送の効率も高く保たれる。

【0018】前記記憶手段は、暗号化済みの前記転送対象データを、暗号化された当該転送対象データに固有の暗号化データ用署名データと対応付けて記憶する手段を備え、前記本体側認証部は、前記カートリッジ側認証部から取得したカートリッジ側署名データが前記カートリッジ側認証部に固有のものであると判別したとき、前記カートリッジ側認証部から前記暗号化データ用署名データを取得し、取得した前記暗号化データ用署名データが、当該暗号化データ用署名データに対応付けられた暗号化済みの前記転送対象データに固有のものであるか否かを判別して、固有のものであると判別したとき、当該暗号化データ用署名データに対応付けられた暗号化済みの前記転送対象データを取得して復号化する手段を備えるものであってもよい。

【0019】これにより、個々の転送対象データが個別に署名による認証の対象とされ、従って転送の可否が個別に決定される。このためデータの秘匿性は更に向上し、更に、個々の転送対象データの重要性の差などに応じて、互いに異なる水準の秘匿性が提供される。

【0020】前記記憶手段は、自己が有する記憶領域のうち暗号化済みの前記転送対象データを記憶する部分の論理的位置を識別する位置データを記憶する手段を備え、前記特定のデータは当該位置データを含んでおり、前記本体側認証部は、前記記憶手段が有する記憶領域のうち前記位置データにより識別される論理的位置から暗

号化済みの前記転送対象データを取得して復号化する手段を備えるものであってもよい。

【0021】これにより、位置データの不正な書き換えが実質的に不可能となる結果、暗号化された転送対象データをカートリッジ側認証部に不正に書き込むことが実質的に不可能となり、従って、転送対象データが不正に書き換えられる危険が避けられる。なお、位置データ自体の大きさは転送対象データに比べて無視し得る程度に小さいのが通常であるから、データの転送の効率は損なわれない。

【0022】前記記憶手段は、自己が有する記憶領域のうち暗号化済みの前記転送対象データを記憶する部分の論理的位置を識別する位置データを記憶する手段と、前記位置データに固有の位置データ用署名データを記憶する手段と、を備え、前記本体側認証部は、前記カートリッジ側認証部から前記位置データ用署名データを取得し、取得した前記位置データ用署名データが前記位置データに固有のものであるか否かを判別して、固有のものであると判別したとき、前記記憶手段が有する記憶領域のうち前記位置データにより識別される論理的位置から暗号化済みの前記転送対象データを取得して復号化する手段を備えるものしてもよい。これによても、位置データの不正な書き換えが実質的に不可能となる結果、転送対象データが不正に書き換えられる危険が避けられる。

【0023】また、この発明の第2の観点にかかる認証装置は、転送対象データを記憶する記憶手段と、特定のデータ、及び当該特定のデータを所定の一方向性関数に代入した値を表すダイジェストを秘密鍵を用いて暗号化したものと表すカートリッジ側署名データを記憶するカートリッジ側記憶手段と、自己に接続された装置から本体側署名データを取得して、その本体側署名データが当該装置に固有のものであるか否かを判別し、固有のものであると判別したとき、前記記憶手段が記憶している前記転送対象データを当該装置に供給するカートリッジ側判別手段と、を備えるカートリッジ側認証装置に着脱可能に接続される認証装置であって、自己に固有の前記本体側署名データを記憶する本体側記憶手段と、前記カートリッジ側認証装置から前記特定のデータを取得し、前記カートリッジ側署名データを公開鍵を用いて復号化し、復号化された前記カートリッジ側署名データが前記ダイジェストと実質的に同一のものであるか否かを判別して、実質的に同一のものであると判別したとき、前記カートリッジ側認証装置から前記転送対象データを取得する本体側判別手段と、を備える、ことを特徴とする。

【0024】このような認証装置は、カートリッジ側認証装置との間で、互いが正規に製造されたものであることを認証した上で、転送対象データの送受を行う。また、カートリッジ側署名データの正当性も検証される。従って、カートリッジ側署名データの作成や秘密鍵の入手を許されていない者から転送対象データが供給されることが阻止される。

手を許されていない者から転送対象データが供給されることが阻止される。

【0025】また、この発明の第3の観点にかかる認証装置は、自己に固有の本体側署名データを記憶する本体側記憶手段と、特定のデータ、及び当該特定のデータを所定の一方向性関数に代入した値を表すダイジェストを秘密鍵を用いて暗号化したものと表すカートリッジ側署名データを記憶する装置から前記カートリッジ側署名データ及び前記特定のデータを取得して、取得した前記カートリッジ側署名データを公開鍵を用いて復号化し、復号化された前記カートリッジ側署名データが前記ダイジェストと実質的に同一のものであるか否かを判別して、実質的に同一のものであると判別したとき、前記装置から転送対象データを取得する本体側判別手段と、を備える本体側認証装置に着脱可能に接続される認証装置であって、前記転送対象データを記憶する記憶手段と、前記カートリッジ側記憶手段と、前記本体側認証装置から前記本体側署名データを取得して、その本体側署名データが前記本体側認証装置に固有のものであるか否かを判別し、固有のものであると判別したとき、前記記憶手段が記憶している前記転送対象データを前記本体側認証装置に供給するカートリッジ側判別手段と、を備える、ことを特徴とする。

【0026】このような認証装置は、本体側認証装置との間で、互いが正規に製造されたものであることを認証した上で、転送対象データの送受を行う。また、カートリッジ側署名データの正当性も検証される。従って、カートリッジ側署名データの作成や秘密鍵の入手を許されていない者から転送対象データが供給されることが阻止される。

【0027】また、この発明の第4の観点にかかる認証システムは、第1及び第2の認証部を備え、前記第1の認証部は、自己に固有の第1の署名データを記憶する第1の記憶手段と、前記第2の認証部から特定のデータを取得し、第2の署名データを公開鍵を用いて復号化し、復号化された前記第2の署名データが、特定のデータを所定の一方向性関数に代入した値を表すダイジェストと実質的に同一のものであるか否かを判別して、実質的に同一のものであると判別したとき、前記第2の署名データが前記第2の認証部に固有のものであるか否かを判別し、固有のものであると判別したとき、前記第2の認証部から転送対象データを取得する第1の判別手段と、を備え、前記第2の認証部は、前記転送対象データ及び前記第2の署名データを記憶する第2の記憶手段と、前記第1の認証部から前記第1の署名データを取得して、その第1の署名データが前記第1の認証部に固有のものであるか否かを判別し、固有のものであると判別したとき、前記第2の記憶手段が記憶している前記転送対象データを前記第1の認証部に供給する第2の判別手段と、

を備え、前記第2の署名データは、前記転送対象データのうちの予め特定された部分を表す前記特定のデータを所定の一方向性関数に代入した値を秘密鍵を用いて暗号化したものを表す、ことを特徴とする。

【0028】このような認証システムによれば、第1及び第2の認証部は、互いが正規に製造されたものであることを認証した上で、転送対象データの送受を行う。従って、第2の署名データの作成や秘密鍵の入手を許されていない者から転送対象データが供給されることが阻止される。

【0029】前記第2の記憶手段は、暗号化済みの前記転送対象データを記憶する手段を備え、前記第1の認証部は、前記第2の認証部から取得した第2の署名データが前記第2の認証部に固有のものであると判別したとき、暗号化済みの前記転送対象データを前記第2の認証部から取得して復号化する手段を備えるものであってもよい。これにより、暗号化された転送対象データについては、その秘匿性が更に向上する。また、転送対象データのうち、当該データの利用価値に影響を及ぼす部分を虫食い式に暗号化するなどすれば、データの転送の効率も高く保たれる。

【0030】前記第2の記憶手段は、暗号化済みの前記転送対象データを、暗号化された当該転送対象データに固有の暗号化データ用署名データと対応付けて記憶する手段を備え、前記第1の認証部は、前記第2の認証部から取得した第2の署名データが前記第2の認証部に固有のものであると判別したとき、前記第2の認証部から前記暗号化データ用署名データを取得し、取得した前記暗号化データ用署名データが、当該暗号化データ用署名データに対応付けられた暗号化済みの前記転送対象データに固有のものであるか否かを判別して、固有のものであると判別したとき、当該暗号化データ用署名データに対応付けられた暗号化済みの前記転送対象データを取得して復号化する手段を備えるものであってもよい。これにより、個々の転送対象データが個別に署名による認証の対象とされ、従って転送の可否が個別に決定される。このためデータの秘匿性は更に向上し、更に、個々の転送対象データの重要性の差などに応じて、互いに異なる水準の秘匿性が提供される。

【0031】また、この発明の第5の観点にかかるコンピュータ読み取り可能な記録媒体は、転送対象データを記憶する記憶手段と、特定のデータ、及び当該特定のデータを所定の一方向性関数に代入した値を表すダイジェストを秘密鍵を用いて暗号化したものを表すカートリッジ側署名データを記憶するカートリッジ側記憶手段と、自己に接続された装置から本体側署名データを取得して、その本体側署名データが当該装置に固有のものであるか否かを判別し、固有のものであると判別したとき、前記記憶手段が記憶している前記転送対象データを当該装置に供給するカートリッジ側判別手段と、を備えるカ

ートリッジ側認証装置に着脱可能に接続されたコンピュータを、自己に固有の前記本体側署名データを記憶する本体側記憶手段と、前記カートリッジ側認証装置から前記特定のデータを取得し、前記カートリッジ側署名データを公開鍵を用いて復号化し、復号化された前記カートリッジ側署名データが前記ダイジェストと実質的に同一のものであるか否かを判別して、実質的に同一のものであると判別したとき、前記カートリッジ側認証装置から前記転送対象データを取得する本体側判別手段と、して機能させるためのプログラムを記録したことを特徴とする。

【0032】このような記録媒体に記録されたプログラムを実行するコンピュータは、カートリッジ側認証装置との間で、互いが正規に製造されたものであることを認証した上で、転送対象データの送受を行う。また、カートリッジ側署名データの正当性も検証される。従って、カートリッジ側署名データの作成や秘密鍵の入手を許されていない者から転送対象データが供給されることが阻止される。

【0033】また、この発明の第6の観点にかかるコンピュータ読み取り可能な記録媒体は、自己に固有の本体側署名データを記憶する本体側記憶手段と、特定のデータ、及び当該特定のデータを所定の一方向性関数に代入した値を表すダイジェストを秘密鍵を用いて暗号化したものと表すカートリッジ側署名データを記憶する装置から前記カートリッジ側署名データ及び前記特定のデータを取得して、取得した前記カートリッジ側署名データを公開鍵を用いて復号化し、復号化された前記カートリッジ側署名データが前記ダイジェストと実質的に同一のものであるか否かを判別して、実質的に同一のものであると判別したとき、前記装置から転送対象データを取得する本体側判別手段と、を備える本体側認証装置に着脱可能に接続されたコンピュータを、前記転送対象データを記憶する記憶手段と、前記カートリッジ側署名データ及び前記特定のデータを記憶するカートリッジ側記憶手段と、前記本体側認証装置から前記本体側署名データを取得して、その本体側署名データが前記本体側認証装置に固有のものであるか否かを判別し、固有のものであると判別したとき、前記記憶手段が記憶している前記転送対象データを前記本体側認証装置に供給するカートリッジ側判別手段と、して機能させるためのプログラムを記録したことを特徴とする。

【0034】このような記録媒体に記録されたプログラムを実行するコンピュータは、本体側認証装置との間で、互いが正規に製造されたものであることを認証した上で、転送対象データの送受を行う。また、カートリッジ側署名データの正当性も検証される。従って、カートリッジ側署名データの作成や秘密鍵の入手を許されていない者から転送対象データが供給されることが阻止される。

【0035】

【発明の実施の形態】この発明の実施の形態にかかる認証システム及び認証装置を、ゲーム機と、そのゲーム機が実行するゲーム用ソフトウェアを記憶するカセットとを含んだゲームシステムを例として説明する。

【0036】図1は、このゲームシステムの構成を示す図である。図示するように、このゲームシステムは、ゲーム機1と、カセット2と、出力装置3とからなる。

【0037】ゲーム機1は、制御部11と、主記憶部12と、外部記憶部13と、入力部14と、スロット15と、インターフェース16と、認証用LSI(Large Scale Integrated circuit)17とからなる。制御部11は、内部バスを介して、主記憶部12、外部記憶部13、入力部14、インターフェース16及び認証用LSI17に接続されており、インターフェース16はスロット15に接続されている。また、制御部11は出力装置3に接続されている。

【0038】制御部11は、CPU(Central Processing Unit)等からなり、カセット2からインターフェース16を介して供給されるプログラムデータが表すゲームプログラムを実行する。また、制御部11は、外部記憶部13が記憶するプログラムデータを読み出して、そのプログラムデータが表すプログラムに従った後述の処理を実行する。

【0039】主記憶部12は、RAM(Random Access Memory)等からなり、制御部11の作業領域として用いられる。外部記憶部13はROM(Read Only Memory)等からなり、制御部11が実行すべき処理を表すプログラムデータを記憶する。

【0040】入力部14は、ジョイスティック等からなり、ユーザの操作に従った信号を制御部11に供給する。スロット15は、カセット2のインターフェース22を着脱可能に装着することにより、ゲーム機1のインターフェース16と、カセット2のインターフェース22とを互いに接続する。

【0041】インターフェース16は、カセット2のインターフェース22から供給されるシリアル形式のデータをパラレル形式のデータに変換して制御部11や認証用LSI17に供給する。また、インターフェース16は、制御部11から供給されるパラレル形式のデータをシリアル形式のデータに変換してインターフェース22に供給する。

【0042】認証用LSI17は、ASIC(特定用途向け集積回路)等からなり、後述する処理に従って、後述するダイジェストの計算や乱数の発生を行い、得られたダイジェストや乱数を制御部11に供給する。また、認証用LSI17は、後述する処理を実行するために用いる後述の鍵暗号化用の秘密鍵、署名検証用の公開鍵及び共通秘密データを予め記憶している。

【0043】カセット2は、ROM21と、インターフ

エース22と、認証用LSI23とからなる。ROM21及び認証用LSI23は、内部バスを介してインターフェース22に接続されている。そして、ROM21は、ゲーム機1の制御部11の指示に従い、自己が記憶しているデータを出力する。出力されたデータは、カセット2のインターフェース22及びゲーム機1のインターフェース16を介して制御部11に供給される。

【0044】ROM21には、例えば図2に示すように、以下(1)～(6)として示す情報が格納されている。すなわち、ROM21の記憶領域には、(1)ゲーム機1が実行すべきゲームプログラムの一部を表すデータであって、暗号化が施されていないデータである非暗号化モジュールと、(2)ゲーム機1が実行すべきゲームプログラムの一部を表すデータであって、所定の暗号鍵を用いて暗号化したものを表す暗号化モジュールと、(3)暗号化モジュール(つまり上述の(2)の情報)を作成するために用いた上述の暗号鍵を所定の鍵暗号化用の公開鍵を用いて暗号化したものと表す暗号化暗号鍵と、(4)ROM21の記憶領域中、各々の暗号化モジュールが格納されている記憶領域を特定する情報(例えば、その記憶領域に付されたアドレス等)を表す暗号化位置リストと、(5)ROM21の記憶領域中、デジタル署名の対象である記憶領域を特定する情報(例えば、その記憶領域に付されたアドレス等)を表す署名対象リストと、(6)署名対象リスト(つまり上述の(5)の情報)が表す記憶領域に格納されているデータ全体を所定の規則に従って結合したものを所定のハッシュ関数に代入した値(すなわち、「ダイジェスト」)を、署名用の秘密鍵で暗号化したものと表す署名データと、が、カセット2の供給者などにより予め格納されている。

【0045】なお、(2)の情報を作成するために用いる暗号鍵は任意のものであってよく、例えば、アメリカ合衆国が定める規格であるDES(Data Encryption Standard)に準拠したものであればよい。また、当該暗号鍵を暗号化するために用いた鍵暗号化用の公開鍵と対をなす鍵復号化用の秘密鍵は、ゲーム機1の認証用LSI17に記憶されている。また、(6)のデータの作成に用いられる上述のダイジェストは、実質的にハッシュ関数として扱い得る任意の関数を用いて作成されればよく、当該関数は、例えばSHA(Secure Hash Algorithm)に準拠したものであればよい。

【0046】そして、上述の署名用の秘密鍵と対をなす署名検証用の公開鍵は、ゲーム機1の認証用LSI17に記憶されている。ただし、署名用の秘密鍵は、(3)の情報を作成するために用いた鍵暗号化用の公開鍵と対になる鍵復号化用の秘密鍵とは別個のものである。

【0047】署名データの作成のためにデジタル署名の対象とされるデータ(すなわち、署名対象リストが示す記憶領域に格納されているデータ)は、カセット2の

供給元等により予め指定される。デジタル署名の対象のデータを指定する基準としては、具体的には、例えば、認証用LSI17が後述する処理に従ってデジタル署名の対象のデータを取得してから当該データのダイジェストを算出するまでの所要時間が一定時間以内となるように、当該データの指定を行うものとすればよい。これにより、後述する署名確認の処理の速度が一定速度以上に保たれ、従って、このゲームシステムによるゲームの円滑な進行が確保される。

【0048】ただし、暗号化位置リスト（すなわち、上述の（4）の情報）は、暗号化モジュールがROM21に1個も格納されておらず従って暗号化位置リストが存在しない、という場合を除き、デジタル署名の対象とされているものとする。従って、ROM21に暗号化位置リストが格納されている限り、署名対象リストには、暗号化位置リストが格納されている記憶領域を特定する情報が含まれるものとする。

【0049】このように、暗号化位置リストをデジタル署名の内容とすることにより、ROM21に格納されているデータが不正に書き換えられる危険が避けられる。すなわち、署名データを検証するためには、後述するように、署名対象リストにより特定されるデータ全体が用いられる。このため、ROM21に格納されているデータの不正な書き換えにも拘わらずカセット2が認証されるようになるためには、暗号化位置リストを書き換えずに残しておく必要が生じる。従って、データを不正に書き換える者は、ROM21に残される暗号化位置リストが示していない記憶領域には暗号化モジュールを書き込むことができない。このため、実質的に利用価値のあるデータをROM21に不正に書き込むことは、極めて困難となる。

【0050】インターフェース22は、ゲーム機1のインターフェース16から供給されるシリアル形式のデータをパラレル形式のデータに変換して認証用LSI23に供給する。また、インターフェース22は、認証用LSI23から供給されるパラレル形式のデータをシリアル形式のデータに変換してインターフェース16に供給する。

【0051】認証用LSI23は、ASIC等からなり、後述する処理に従ってダイジェストの計算や乱数の発生を行い、得られたダイジェストや乱数をゲーム機1に供給する。また、認証用LSI23は、ゲーム機1の認証用LSI17が記憶しているものと実質的に同一の共通秘密データを予め記憶し、更に、署名データの作成に用いられた上述のダイジェスト（すなわち、署名用の秘密鍵で暗号化することにより上述の（6）の情報となるデータ）を予め記憶している。（なお、以下では、認証用LSI23が予め記憶する上述のダイジェストをダイジェストdAと呼ぶ。）

【0052】出力装置3は、テレビジョン受像機等から

なり、ゲーム機1の制御部11の指示に従った画像を表示し、また、制御部11の指示に従った音声を再生する。

【0053】（動作）次に、このゲームシステムの動作を、図3～図5を参照して説明する。図3は、デジタル署名確認の処理を表すフローチャートである。図4は、相互認証の処理を表すフローチャートである。図5は、ゲームプログラムの実行の手順を表すフローチャートである。

10 【0054】（デジタル署名確認）ゲーム機1は、スロット15にカセット2が装着された上で起動され、ユーザが入力部14を用いてゲームの開始を指示すると、ゲーム機1はこの指示に応答して、まず、図3に示すデジタル署名確認の処理を実行する。

【0055】デジタル署名確認の処理を開始すると、ゲーム機1の制御部11は、インターフェース16及び22を介してカセット2のROM21にアクセスする。そして、ROM21に格納されている署名対象リスト（すなわち上述の（5）の情報）と、当該署名対象リストに対応付けられている署名データとを読み込み、認証用LSI17に供給する（図3、ステップS101）。

【0056】認証用LSI17は、制御部11から署名対象リスト及び署名データを供給されると、署名データの作成のための暗号化の対象とされたデータを、ROM21に格納されている署名データを作成するために用いたものと実質的に同一のハッシュ関数に代入した値（以下、この値をダイジェストdBと呼ぶ）を計算し、ダイジェストdBを制御部11に供給する（ステップS102）。

30 【0057】なお、署名データの作成のための暗号化の対象とされたデータは、具体的には、上述のように、署名対象リストが表す記憶領域に格納されているデータ全体である。そして、ステップS102において認証用LSI17は、例えば、署名対象リストが表す記憶領域にある各データを所定の規則に従って互いに結合して1個のデータを作成し、作成したデータにつきダイジェストdBを計算する。

【0058】次に、認証用LSI17は、ステップS101で供給された署名データを、自己が記憶する署名検証用の公開鍵を用いて復号化し、復号化の結果生成されたデータ（復号化済み署名データ）を主記憶部12に格納する（ステップS103）。

【0059】制御部11は、ステップS102で認証用LSI17から供給されたダイジェストdBと、ステップS103で認証用LSI17が生成して主記憶部12に格納した復号化済み署名データとが、実質的に一致するか否かを判別する（ステップS104）。そして、一致しないと判別すると、出力装置3に、認証の失敗を表す画像の表示を指示して、処理を終了し、出力装置3は、この指示に応答して、認証の失敗を表す画像を表示

する。

【0060】(相互認証の処理)一方、ステップS104において、ダイジェストdBと復号化済み署名データとが実質的に一致すると判別すると、制御部11は、図4に示す相互認証の処理を実行する。

【0061】相互認証の処理を開始すると、制御部11は、認証用LSI17に、認証の開始を指示する。認証用LSI17はこの指示に応答して乱数を生成し、生成した乱数をチャレンジデータとして、インターフェース16及び22を介し、カセット2の認証用LSI23に供給する(図4、ステップS201)。

【0062】認証用LSI23は、認証用LSI17よりチャレンジデータを供給されると、そのチャレンジデータ、自己が記憶する共通秘密データ及び自己が予め記憶するダイジェストdA(署名用の秘密鍵で暗号化されれば署名データとなるダイジェスト)の三者を所定の手法により互いに結合して1個のデータを作成する(図4、ステップS301)。

【0063】そして、作成したデータを、所定のハッシュ関数(例えば、ステップS102で用いたものと実質的に同一のハッシュ関数)に代入した値(以下、この値をダイジェストdCと呼ぶ)を計算する(ステップS302)。ステップS302でダイジェストdCが算出されると、認証用LSI23は、ダイジェストdCをレスポンスデータとして、インターフェース22及び16を介し、ゲーム機1の認証用LSI17に供給する(ステップS303)。

【0064】認証用LSI17は、カセット2の認証用LSI23からレスポンスデータを供給されると、ステップS201で自己が供給したチャレンジデータ、自己が記憶する共通秘密データ、及び署名確認の処理のステップS103において主記憶部12に格納された復号化済み署名データの三者を互いに結合して1個のデータを作成する(ステップS202)。

【0065】そして、認証用LSI17は、ステップS202で作成されたデータのダイジェスト(以下、ダイジェストdDと呼ぶ)を、ステップS302で用いたものと実質的に同一のハッシュ関数を用いて計算する(ステップS203)。そして、得られたダイジェストdDが、ステップS303で自己に供給されたレスポンスデータ(すなわちダイジェストdC)と実質的に同一のものであるか否かを判別する(ステップS204)。

【0066】ステップS204において、ダイジェストdDとレスポンスデータとが実質的に同一のものであると判別すると、認証用LSI17は、カセット2の認証用LSI23に所定の形式のサクセスマッセージを送る(ステップS205)。認証用LSI23は、ゲーム機1の認証用LSI17からサクセスマッセージを供給されると、このサクセスマッセージに応答して乱数を生成し、生成した乱数をチャレンジデータとして、認証用L

SI17に供給する(ステップS304)。

【0067】一方、ステップS204において、一致しないと判別すると、認証用LSI17は、ゲーム機1の制御部11に、認証の失敗を通知する。制御部11は、認証の失敗を表す画像の表示を出力装置3に指示して処理を終了し、出力装置3は、この指示に応答して、認証の失敗を表す画像を表示する。

【0068】認証用LSI17は、ステップS304で認証用LSI23よりチャレンジデータを供給されると、そのチャレンジデータ、自己が記憶する共通秘密データ、及びステップS103で主記憶部12に格納された復号化済み署名データの三者を所定の手法により互いに結合して1個のデータを作成する(ステップS206)。

【0069】そして、ステップS206で作成されたデータのダイジェスト(ダイジェストdE)を、ステップS302で用いたものと実質的に同一のハッシュ関数を用いて計算し、得られたダイジェストdEをレスポンスデータとしてカセット2の認証用LSI23に供給する(ステップS207)。

【0070】認証用LSI23は、ステップS207でゲーム機1からレスポンスデータを供給されると、ステップS304で自己が供給したチャレンジデータ、共通秘密データ、及び自己が予め記憶するダイジェストの三者を互いに結合して1個のデータを作成する(ステップS305)。

【0071】そして、認証用LSI23は、ステップS305で作成されたデータのダイジェスト(ダイジェストdF)を、ステップS302で用いたものと実質的に同一のハッシュ関数を用いて計算する(ステップS306)。そして、得られたダイジェストdFが、ステップS207で自己に供給されたレスポンスデータ(すなわちダイジェストdE)と実質的に一致するか否かを判別する(ステップS307)。

【0072】ステップS307において、一致しないと判別すると、認証用LSI17は、制御部11に認証の失敗を通知する。制御部11は、認証の失敗を表す画像の表示を出力装置3に指示して処理を終了し、出力装置3は、この指示に応答して、認証の失敗を表す画像を表示する。

【0073】一方、ステップS307において、ダイジェストdFとレスポンスデータとが実質的に一致すると判別すると、認証用LSI23は、ゲーム機1の認証用LSI17に所定の形式のサクセスマッセージを送り(ステップS308)、相互認証の処理を終了する。ステップS308でサクセスマッセージを供給された認証用LSI17は、制御部11に認証の成功を通知し(ステップS208)、相互認証の処理を終了する。

【0074】(ゲームプログラムの実行)制御部11が認証の成功の通知を供給されると、このゲームシステム

は、引き続き、図5に示す手順でゲームプログラムを実行する。

【0075】まず、制御部11は、ROM21から暗号化暗号鍵を読み出して、認証用LSI17に供給する。認証用LSI17は、自己が記憶する鍵復号化用の秘密鍵を用いて暗号化暗号鍵を復号化し、復号化により得られた暗号鍵を制御部11に供給する(図5、ステップS401)。暗号鍵を供給された制御部11は、ROM21より暗号化位置リストを読み込む(ステップS402)。

【0076】次に、制御部11は、ROM21に格納されているデータのうち、ゲームプログラムの最初の処理を表すものを特定し、読み込む(ステップS403)。最初の処理の特定は任意の手法で行ってよく、例えば、最初の処理を表すデータに予め所定の形式のヘッダをしておき、制御部11がROM21に格納されたデータのうちから当該ヘッダを索出するようにすればよい。

【0077】次に、制御部11は、ステップS402で読み込んだ暗号化位置リストの内容を解析することにより、ステップS403で読み込んだデータが暗号化モジュールであるか否かを判別する(ステップS404)。そして、暗号化モジュールでなければ(非暗号化モジュールであれば)、当該非暗号化モジュールが表す処理を実行する(ステップS405)。暗号化モジュールであれば、ステップS401で自己に供給された暗号鍵を用いて当該暗号化モジュールを復号化し(ステップS406)、復号化により得られたデータが表す処理を実行する(ステップS407)。

【0078】そして、ステップS405やS407で実行した処理において、他の処理が呼び出されると、制御部11は、呼び出された処理を表すデータを読み出し、そのデータをステップS403で特定されたデータとして扱い、ステップS404に処理を移す。

【0079】すなわち、制御部11は、ステップS405やS407で呼び出された処理を表すデータを読み込み、暗号化位置リストの内容に基づいて、読み込んだデータが暗号化モジュールであるか否かを判別する。そして、暗号化モジュールでなければステップS405に処理を移し、暗号化モジュールであればステップS406に処理を移す。

【0080】以上説明した処理により、このゲームシステムは、ROM21に格納されているデータに従ってゲームプログラムを実行する。その際、実行すべき対象の処理を表すデータが暗号化されている場合は、そのデータを復号化した上で当該処理を実行する。

【0081】以上説明したように、このゲームシステムでは、実行する対象のゲームプログラムの全体を署名の対象とする必要はなく、例えば、ゲームプログラムの一部を署名データ作成に用いるようにすれば、当該ゲームプログラムを不正なアクセスから保護する目的が実質的

に達成される。

【0082】そして、上述のように、ゲームプログラムの一部を署名の対象とすれば(すなわち、虫食い式に署名を行えば)、ゲームプログラム全体を署名の対象とした場合に比べダイジェストの計算が高速になる結果、署名確認の処理が高速になり、ゲームの円滑な進行が阻害されにくくなる。

【0083】また、このゲームシステムでは、実行する対象のゲームプログラムの全体を暗号化する必要はなく、例えば、ゲームの進行上重要な場面の処理を表すデータを暗号化すれば、当該ゲームプログラムを不正なアクセスから保護する目的が実質的に達成される。

【0084】そして、上述のように、ゲームプログラムを部分的に(虫食い式に)暗号化すれば、ゲームプログラム全体を暗号化した場合に比べ、ゲームプログラムの実行が高速になり、ゲームの円滑な進行が阻害されにくくなる。また、暗号化の省略の結果、ROM21に格納する情報の冗長性が小さくなり、ROM21へのデータの格納が効率的になる。

【0085】なお、このゲームシステムの構成は、上述のものに限られない。例えば、ROM21が記憶するデータはゲーム機1が実行するゲームのプログラムを表すものである必要はないし、ゲーム機1もゲームプログラムを実行するための装置である必要はない。また、カセット2はゲーム機1に供給する対象のデータをROM21に格納する必要はなく、ゲーム機1に供給する対象のデータは、例えばCD-ROMやDVD(Digital Video Disk)や、その他任意の記録媒体に格納されていてよい。また、ゲーム機1とカセット2とが互いに着脱可能に接続される必要はなく、両者は互いに固定的に接続されていてもよいし、通信回線を介して相互にデータの交換を行うものであってもよい。

【0086】また、認証用LSI17の機能を制御部11が行ってもよいし、複数の集積回路が認証用LSI17の機能を行うようにしてもよいし、複数の集積回路が認証用LSI23の機能を行うようにしてもよい。また、ステップS406でデータの復号化に用いる暗号鍵は、予めゲーム機1が記憶していてもよい。

【0087】また、カセット2の認証用LSI23が有する、ダイジェストdAを記憶する記憶領域は、例えば、PROM(Programmable Read Only Memory)等の1回書き込み可能な不揮発性記憶装置が有する記憶領域であってもよい。この場合、認証用LSI23は、ROM21に格納されるデータが異なるカセット2毎に個別に製造する必要はない。従って、例えば、1回書き込み可能な記憶領域の内容が初期化された状態の認証用LSI23を量産し、その後、個々の認証用LSI23の1回書き込み可能な記憶領域にダイジェストdAを書き込むようにしてもよい。

【0088】また、ゲーム機1の認証用LSI17が有

する、鍵暗号化用の秘密鍵、署名検証用の公開鍵を記憶する記憶領域は、EEPROM (Electrically Erasable/Programmable Read Only Memory) 等の書き換え可能な不揮発性記憶装置が有する記憶領域であってもよい。この場合、認証用LSI17は、カセット2から取得するデータが異なるもの毎に個別に製造する必要はなく、例えば、書き換え可能な記憶領域の内容が初期化された状態の認証用LSI17を量産してもよい。そして、書き換え可能な記憶領域の内容が初期化された認証用LSI17を備えるゲーム機1のユーザ等が、そのゲーム機1に接続する予定のカセット2を認証するために必要な署名検証用の公開鍵などを、そのゲーム機1の認証用LSI17の書き換え可能な記憶領域に書き込むようにしてもよい。

【0089】また、ROM21は、暗号化モジュールと対応付けて、上述の署名データとは別個の暗号化モジュール用署名データを格納するようにしてもよい。暗号化モジュール用署名データは、例えば、自己に対応付けられている暗号化モジュールを、上述の署名用の秘密鍵や鍵復号化用の秘密鍵とは別個の第3の秘密鍵を用いて暗号化したものであればよい。この場合、例えば認証用LSI17が、当該第3の秘密鍵と対をなす第3の公開鍵を予め記憶するようにすればよい。

【0090】これにより、暗号化モジュールの秘匿性は更に向かう。また、例えば、カセット2のROM21に格納したゲームプログラムのプログラムデータのうち、試用版のゲームの処理を表す部分以外を個別に署名の対象とし、第3の公開鍵を記憶していないゲーム機1を用いて試用版のゲームを行うことができるようになる、等の応用が可能となる。

【0091】暗号化モジュールに暗号化モジュール用署名データが対応付けられている場合、このゲームシステムは、制御部11に認証の成功の通知が供給された後、例えば図6に示す手順でゲームプログラムを実行すればよい。図6に示す手順において、図5に示すものと同一の参照番号を付した処理は、図5に示すものと実質的に同一の処理を表すものである。

【0092】すなわち、制御部11が認証の成功の通知を供給されると、このゲームシステムは、引き続き、図5のステップS401～S404と実質的に同一の処理を行う(図6、ステップS401～S404)。図6のステップ404の処理(つまり、図5のステップ404と実質的に同一の処理)において、ステップS403で特定されたデータが暗号化モジュールであると判別したとき、制御部11は、そのデータに対応付けられている暗号化モジュール用署名データがあるか否かを判別する(ステップS408)。

【0093】そして、ないと判別したとき、制御部11は処理をステップS406に移す。あると判別したときは、該当する暗号化モジュール用署名データを読み込

み、読み込んだ暗号化モジュール用署名データと、ステップS403で読み込んだ暗号化モジュールとを、認証用LSI17に供給する(ステップS409)。

【0094】認証用LSI17は、制御部11から供給された暗号化モジュールを、所定のハッシュ関数(例えば、ステップS102で用いたものと実質的に同一のハッシュ関数に代入した値(以下、ダイジェストdGと呼ぶ)を計算し、ダイジェストdGを制御部11に供給する(ステップS410)。

10 【0095】次に、認証用LSI17は、ステップS409で供給された暗号化モジュール用署名データを、自己が記憶する第3の公開鍵を用いて復号化し、復号化により得られたデータを制御部11に供給する(ステップS411)。

【0096】次に、制御部11は、ステップS410で認証用LSI17から供給されたダイジェストdGと、ステップS411で認証用LSI17から供給されたデータとが実質的に一致するか否かを判別する(ステップS412)。そして、一致すると判別すると処理をステップS406に移し、一致しないと判別すると、出力装置3に、認証の失敗を表す画像の表示を指示して、ゲームプログラムの実行を終了し、出力装置3は、この指示に応答して、認証の失敗を表す画像を表示する。

【0097】また、暗号化位置データには、上述の署名用の秘密鍵とは別個の暗号化位置データ用の秘密鍵を用いてデジタル署名を施してもよい。この場合、暗号化位置データを署名データ(すなわち、上述の(6)の情報)の作成に用いる必要はなく、従って、署名対象リストには、暗号化位置データが格納されている記憶領域を示す情報が含まれている必要はない。

【0098】暗号化位置データが、暗号化位置データ用の秘密鍵を用いたデジタル署名を施されている場合、例えば、ゲーム機1の認証用LSI17が、暗号化位置データ用の秘密鍵と対をなす暗号化位置データ認証用の公開鍵を記憶していてもよい。そして、ゲーム機1は、例えば上述のステップS402の処理の後、ステップS403の処理に移る前に、暗号化位置データ認証用の公開鍵を用いて、暗号化位置データが、カセット2の正規の供給元により作成されたものであることを認証するようにもよい。

【0099】以上、この発明の実施の形態を説明したが、この発明の認証システム及び認証装置は、専用のシステムによらず、通常のコンピュータシステムを用いて実現可能である。例えば、パーソナルコンピュータに上述の動作を実行するためのプログラムを格納した媒体(フロッピーディスク、CD-ROM等)から該プログラムをインストールすることにより、上述の処理を実行する認証装置及び認証システムを構成することができる。

50 【0100】また、コンピュータにプログラムを供給す

るための媒体は、通信媒体（通信回線、通信ネットワーク、通信システムのように、一時的且つ流動的にプログラムを保持する媒体）でも良い。例えば、通信ネットワークの掲示板（BBS）に該プログラムを掲示し、これをネットワークを介して配信してもよい。そして、このプログラムを起動し、OSの制御下に、他のアプリケーションプログラムと同様に実行することにより、上述の処理を実行することができる。

【0101】なお、OSが処理の一部を分担する場合、あるいは、OSが本願発明の1つの構成要素の一部を構成するような場合には、記録媒体には、その部分をのぞいたプログラムを格納してもよい。この場合も、この発明では、その記録媒体には、コンピュータが実行する各機能又はステップを実行するためのプログラムが格納されているものとする。

【0102】

【発明の効果】以上説明したように、この発明によれば、正規の供給者によるゲーム機及びカートリッジの供給が確保され、データの読み出しやカートリッジの複製が阻止される認証システム及び認証装置が実現される。

【図面の簡単な説明】

【図1】この発明の実施の形態にかかるゲームシステム*

*の基本構成を示すブロック図である。

【図2】ROMに格納されているデータのデータ構造を模式的に示す図である。

【図3】ディジタル署名確認の処理を表すフローチャートである。

【図4】相互認証の処理を表すフローチャートである。

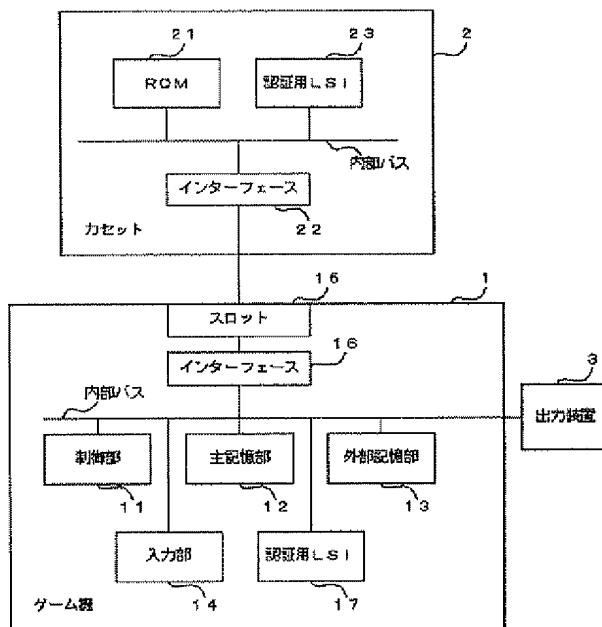
【図5】ゲームプログラムの実行の手順を表すフローチャートである。

【図6】ゲームプログラムの実行の手順の変形例を表すフローチャートである。

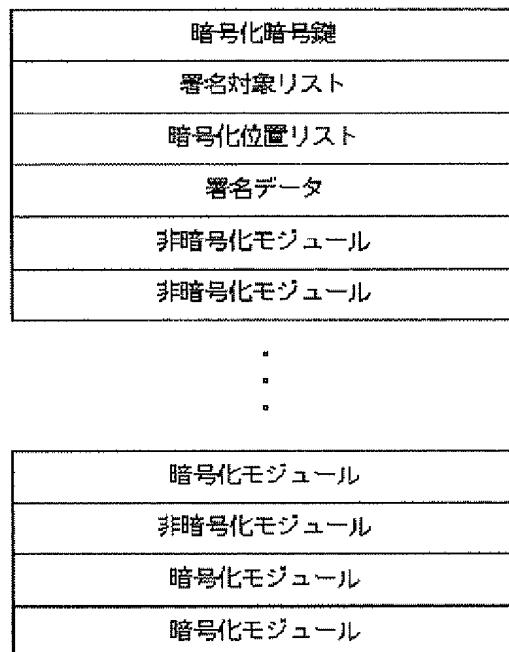
【符号の説明】

1	ゲーム機
1 1	制御部
1 2	主記憶部
1 3	外部記憶部
1 4	入力部
1 5	スロット
1 6、2 2	インターフェース
1 7、2 3	認証用LSI
2	カセット
2 1	ROM

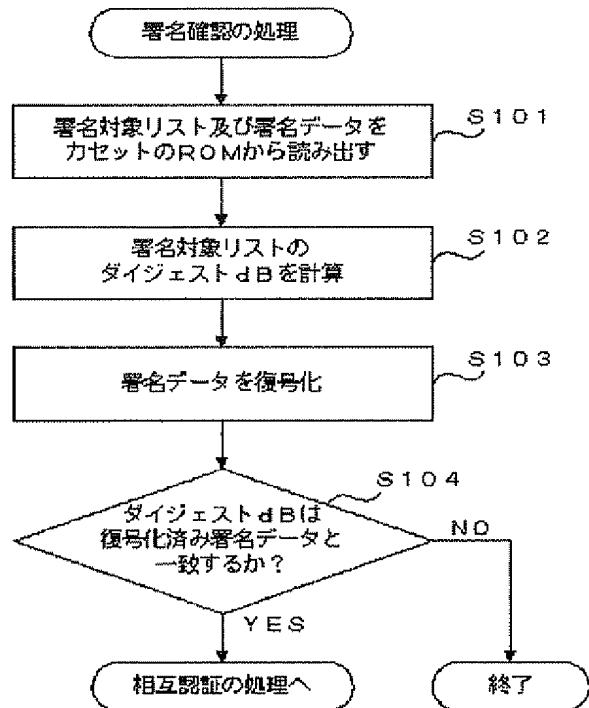
【図1】



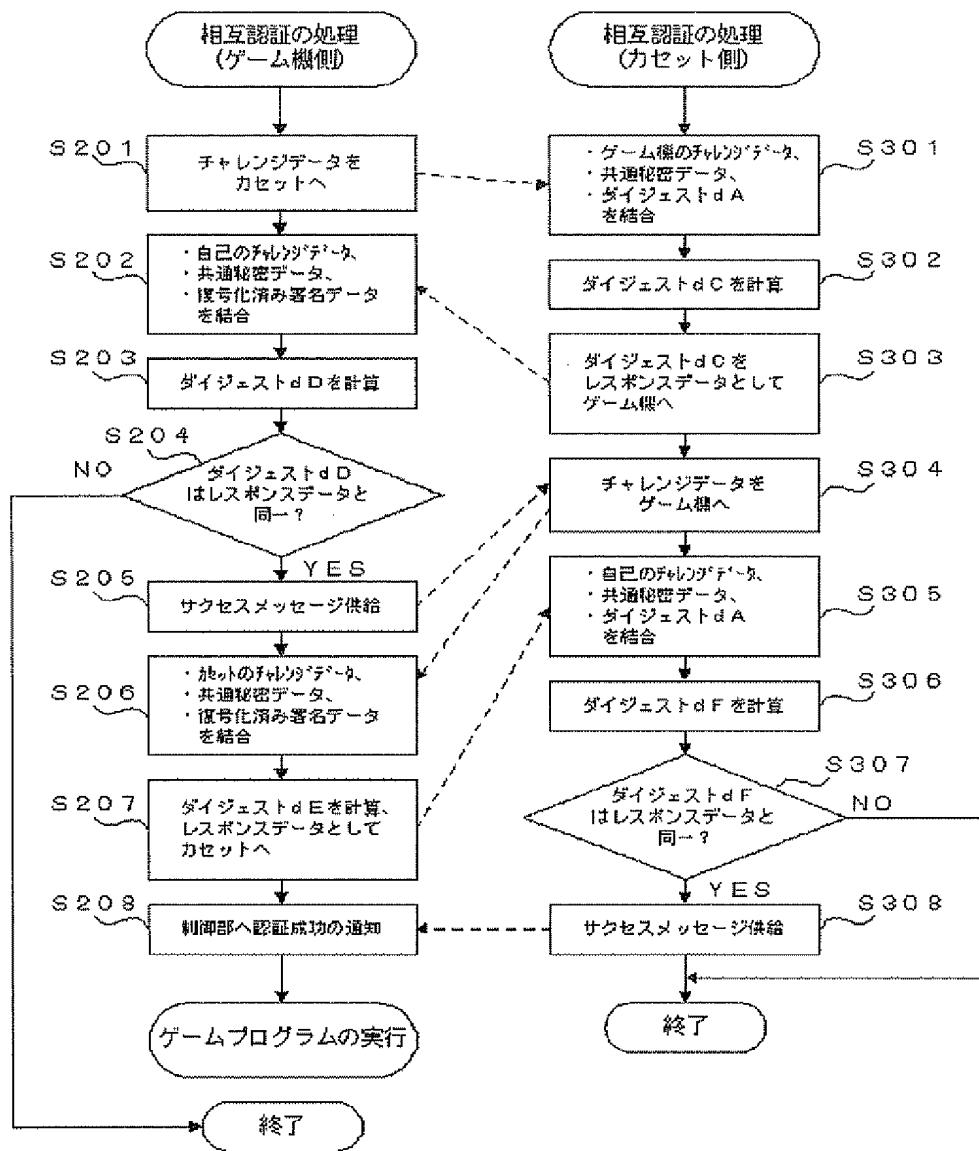
【図2】



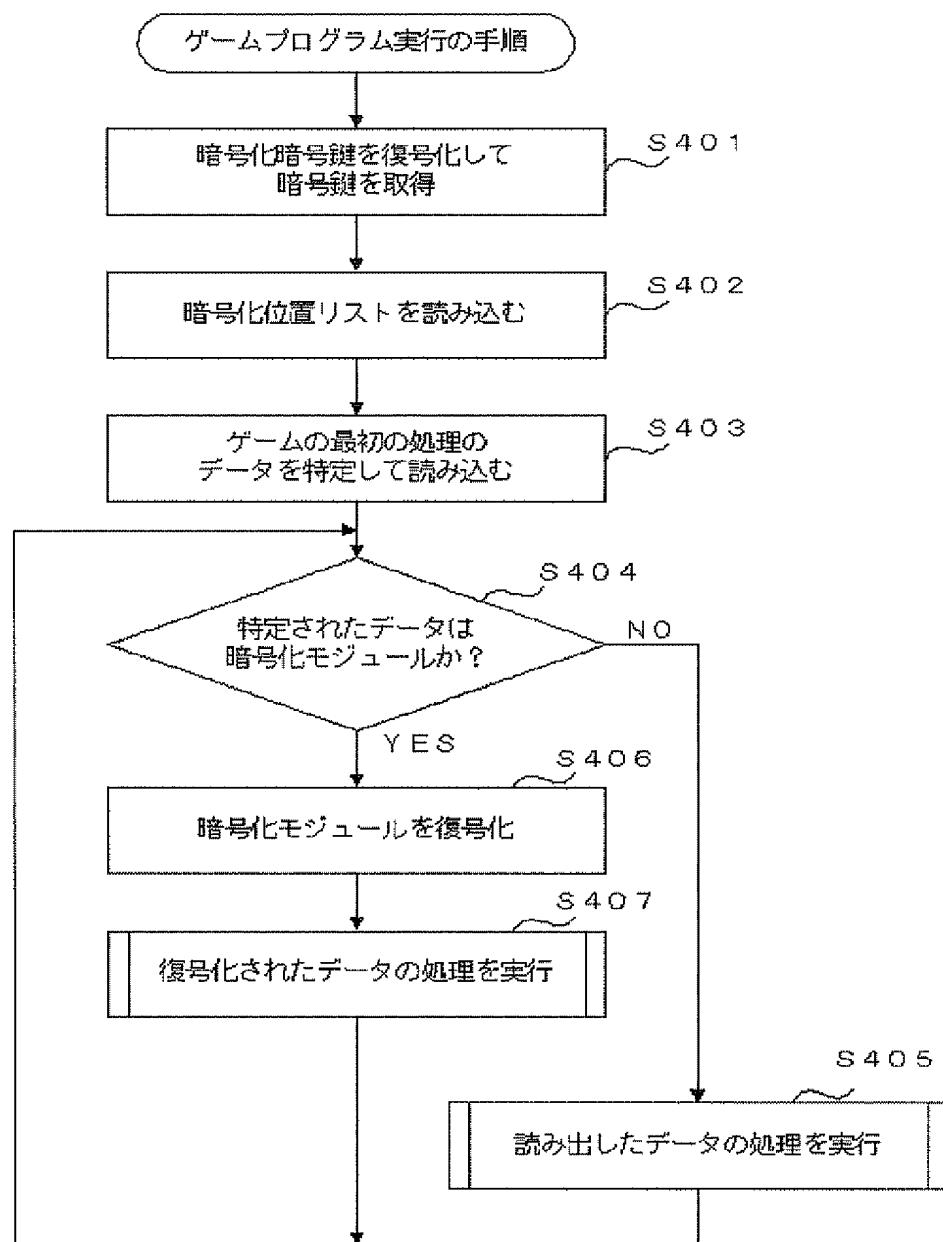
【図3】



【図4】



【図5】



【図6】

